SHIELD

GÜVENLİ YAŞAM REHBERİNİZ

01
Haziran
2018

Evler Artık Daha Güvende!
Akıllı Kilit Sistemi satın almadan önce dikkat etmeniz gerekenler

SHIELD.COM.TR

ÇOCUĞUNUZU YOUTUBE'DAKİ TEHLİKELERDEN KORUMA YÖNTEMLERİ

YouTube çocuklarınız için eğlenceli bir ortam olabilir fakat bu renkli dünya, bazı tehlikeler de barındırıyor. Korunma yöntemlerini anlattık!

Adım Adım
Ev güvenlik sistemi satın alırken bunlara dikkat edin!

Teknoloji
Biyometri teknolojisinin bugünü ve yarınına bakış

Dikkat!
Evlerde yangına karşı alınması gereken 10 tedbir

DOSYA

Otomobil
Lastikler için ideal hava basıncı hakkında bilmeniz gerekenler

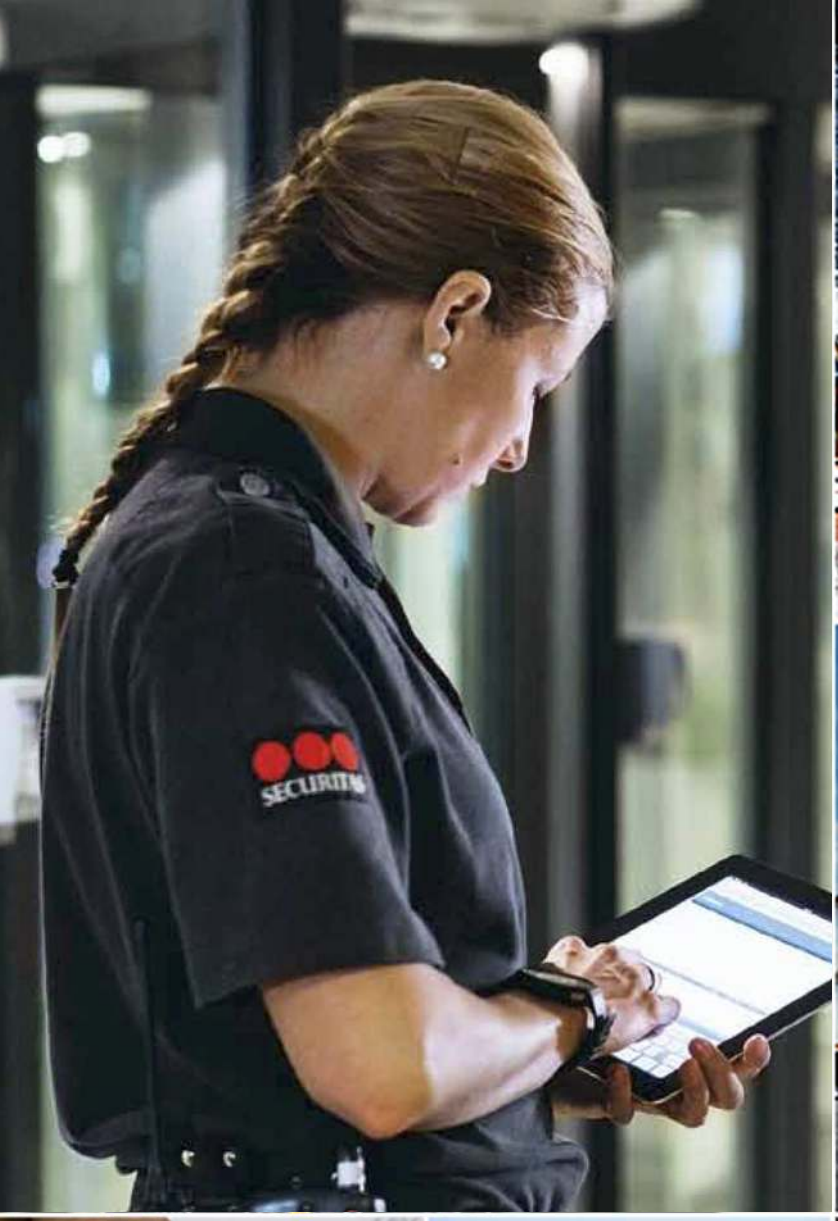
YAŞAM

Sosyal Medya
Ayrılıklar dijital hayatın sınırlarını tehdit ediyor

İŞ HAYATI

Meslek Rehberi
Siber güvenlikçi olmak isteyenlere başlangıç ipuçları

Dergilik
Exclusive



Securitas, segmentinize özel çözümler sunuyor. Bilgi ve teknoloji entegrasyonu ile minimum maliyetle optimum fayda sağlayan çözümleri hayata geçiriyor.

Securitas, 54 ülkede, 345.000 çalışanı ile iş ortaklarının ihtiyaçlarına uygun çözümler üreterek fark yaratıyor.

www.securitas.com.tr

GÜVENLİ YAŞAM REHBERİNİZ

SHIELD'dan

MERHABA!

Ne kadar güvendesiniz? Evde, okulda, iş yerinde, yolda ve gelecekte? Tehditlere karşı kendinizi, sevdiklerinizi ve sahip olduğunuz her şeyi korumak için yapmanız gereken pek çok şey var. Ülkemizde ne yazık ki güvenlik ve emniyet konusunda yeterli farkındalık olduğunu söyleyemiyoruz.

Evinizde ve işyerinizde yangın tüpü, gaz maskesi, duman dedektörü, hırsız alarmı, güvenlik kamerası var mı mesela? Peki ya çocuğunuzun okulunda gerekli emniyet standartları karşılanmış mı?

Eksikliğini, sadece işiniz düştüğünde fark etmek büyük üzüntü ve kayıplar anlamına gelebilir. Bu yüzden tedbiri elden bırakmamak, üşenmemek, "bir şey olmaz" dememek lazım. Daima kötü senaryolara göre tedbirler almalıyız. Güvenlik ve emniyet konularında biraz evhamlı olmanın zararı değil, faydası var.

Saydığım güvenlik ekipmanlarını edinmek hiç de zor değil. Alışveriş sitelerinde çok uygun fiyatlara bulabilirsiniz. Günümüzde bu tür imkanlara erişmek çok daha hızlı, rahat ve ekonomik.

SHIELD'ın misyonu, her anlamda bir güvenlik rehberi oluşturmak. Ülkemizde bu konuda büyük bir ihtiyaç olduğunu düşünüyorum. Bu ilk sayımızda zengin yelpazemizi sizlere sunmaya çalıştık. Sonraki sayılarımızda çok daha fazlasını göreceksiniz.

Böyle bir yayın hazırlamış olmak benim için büyük bir heyecan ve mutluluk sebebi. Bu ay içinde web sitemizi de yayın olarak konumlandıracağız. Yazdan sonra ise SHIELD'ı basılı olarak çıkartmak gibi hedeflerimiz var.

Daha güvenli bir yaşam ve gelecek için SHILD sizlerle. İyi okumalar. Görüşmek üzere!

Erdal Kaplanseren
Yayın Yönetmeni
erdal@layka.com.tr

Sahibi: Layka Medya Yayıncılık ve İletişim Danışmanlığı Dış Tic. Ltd Şti.
Yayın Yönetmeni: Erdal Kaplanseren **Görsel Yönetmen:** Hasan Kaya **Editör:** Hasan Selman

Adres: Muradiye Mah. Kalıpçı Sok. No: 22/8 Beşiktaş/İstanbul **Tel:** 0212 972 9047 **Yazı İşleri:** bilgi@layka.com.tr
Reklam: reklam@layka.com.tr **Yayın Türü:** Yerel, süreli, aylık

© SHIELD dergisi, Layka Medya Yayıncılık ve İletişim Danışmanlığı Dış Tic. Ltd Şti. tarafından T.C. yasalarına uygun olarak yayımlanmaktadır.

İÇİNDEKİLER

Sayı 01 Haziran 2018

Pratik kurulum ve kullanıma sahip ev güvenlik kamerası: Logitech Circle 2

Editörden
3 Güvenli Yaşam Rehberiniz SHIELD'dan Merhaba!

Kapak Konusu
14 Çocuğunuzu YouTube'daki Tehlikelerden Koruyun!

Evde Güvenlik
38 Evlerde Yangına Karşı 10 Tedbir
6 Akıllı Kilit Sistemi Satın Alma Rehberi
12 Ev Güvenlik Sistemi Satın Alırken Bunlara Dikkat Edin!

Sosyal Medya
46 Sosyal Medyada Başınızın Belaya Girmemesi İçin 5 Tavsiye
36 "Kampanya" Tuzaklarına Düşmeyin!

Kariyer
32 Siber Güvenlik Alanında Çalışmak İsteyenler İçin Başlangıç Rehberi

Teknoloji
30 Güvenlikte Yükselen Trend: Biyometri Teknolojisi
40 Parmak İzi Güvenliği Hakkında Doğru Bilinen Yanlışlar

Çocuk Güvenliği
42 Okullar Nano Teknolojiyle Tertemiz
18 Çocukların Güvenli Sosyal Ağ Kullanımı

Finansal Güvenlik
49 Kripto Para Madenciliğinde Büyük Tehlike!

Görüş
44 Özel Güvenlik Çalışanları Haklarını İstiyor

Biyometrik bilgileri kullanmak en güvenli, pratik, hijyenik ve ekonomik yöntem oldu. Biyometri teknolojisini yakından tanıyoruz!

Çocukların güvenli sosyal medya kullanımı için ebeveynlerin yapması gerekenler

İş Yerinde Güvenlik
11 Mağazalar Akıllı Kameralarla Daha Güvenli
50 Securitas'tan Güvenlik 4.0 Açılımı

Geleceğim Güvende
54 Özel Sağlık Sigortası Nedir, Neleri Kapsar, Faydaları Nelerdir?

Kurumsal Güvenlik
39 Kurumsal Siber Güvenlikte %100 Yerli Çözüm: berqNET

Yaşam
28 Ayrılıklar Online Hayatı Tehdit Ediyor
20 Yaşlılar İçin Mobil Güvenlik Sorunu Büyüyor

Kariyer
32 Siber Güvenlik Alanında Çalışmak İsteyenler İçin Başlangıç Rehberi

Yolda Güvenlik
24 Otomobil Lastiklerinde Hava Basıncına Dikkat!

Uygulama
23 Kişisel Güvenliğiniz İçin Mobil Uygulama: Securitas Güvendeyim

Soru-Cevap
10 Temassız Ödeme Güvenli mi?

Ürün İnceleme
9 Hava Koşullarına Dayanıklı Ev Güvenlik Kamerası: Circle 2

Güncel
8 Dijital taksi "Taxi 7x24" ile güvenli yolculuk

Ev güvenlik sistemi satın almak isteyenler için pratik bilgiler

İnternette güvendeyim, annem biliyor :)

ÇOCUK DOSTU EBEVEYN KORUMASI

Çocuklarınız dijital dünyayı keşfederken **ESET Ebeveyn Kontrolü** çocuk merkezli bir yaklaşımla size yardımcı olur.

Ailenizi güvende tutun:

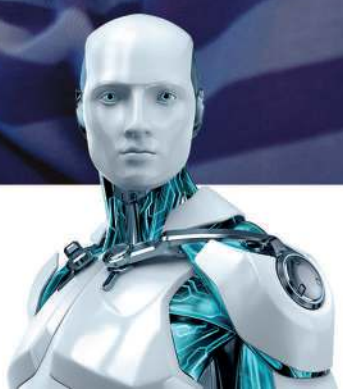
cocuklarguvende.net

eset
ENJOY SAFER TECHNOLOGY™

/ESETTurkiye /ESETTurkiye

ESET Türkiye **www.eset.com.tr** satis@eset.com.tr

İstanbul Merkez: 0212.251 51 80 Ankara: 0312.473 20 74



Akıllı Kilit Sistemi Satın Alma Rehberi

Günümüzde akıllı cihazlar evlerimize nüfuz etmeye başladı. Bu durumdan kapılar da nasibini aldı. Hem yüksek güvenlik, hem de pratik kullanım sunan akıllı kilit sistemlerinden satın almadan önce göz önünde bulundurmanız gereken 5 kriteri derledik.

Dijitalleşme trendinin hayatımızdaki en büyük yansıması akıllı evlerle gerçekleşti. Akıllı televizyonlar, akıllı buzdolapları, akıllı klimalar hatta akıllı perdeler derken kapılarımızdaki kilitler de dijitalleşme trendinden nasibini aldı ve hem daha güvenli hem de daha kullanışlı çözümler sunulmaya başlandı. Ancak doğru akıllı kilit seçme süreci endişe verici olabiliyor. Seçim yapmanız gereken çok fazla özellik, tasarım ve erişim seçeneği var. Teknoloji, basitlik ve konforun bileşimini sunan akıllı anahtarlar tercih edilmeli. Hem şık gözüken, hem de hayatınızı basitleştirirken sizi ve sevdiklerinizi koruyan bir akıllı kilit seçmek için dikkat etmeniz gereken 5 kriteri paylaşıyoruz.

1 Akıllı kilit sisteminin temeli güvenlik, unutmayın

Bazı akıllı kilitler sevimli ve çok şık olabilir ama asıl varlık amaçları güvenliği sağlamaktır. Çoğu kilit benzer prensiplere sahip olsa da, güvenlik düzenlemeleri açısından birbirlerinden ayrılabilir. Almayı düşündüğünüz kilidin sizi ve evinizi gerçekten güvende tutacağına emin olun. Sadece kilidin temel özelliklerine değil, kimlik belirlemeleri ve raporlamaları nasıl yaptığını özenle incelemelisiniz.

2 2- Kurulumunun kolay olmasına dikkat edin

Çoğu kişi akıllı kilit seçerken kapısıyla direkt uyum sağlayıp sağlamayacağını düşünmez. Halbuki bu kritik bir faktördür. Seçeceğiniz kilit kolay bir şekilde kurulmalı ve kapınızda bir değişiklik yapmayı gerektirmemelidir. Kapınızı tamamen değiştirmenizi gerektirecek ya da kapınızın estetiğini bozacak bir kilit, bu çabanıza ya da yeni bir kapıya harcayacağınız paraya değmeyebilir.

3 Kilidin batarya gücünü göz önünde bulundurun

Akıllı kilidinizin şarjının tam ona ihtiyaç duyduğunuz anda bitmesi hayal kırıklığı yaratabilir. Yeni bir batarya almak ya da bataryaları sık sık şarj etmek de rahatsız edicidir. Bu nedenle sürdürülebilir özellikte ve kısa sürede şarj olan bir batarya aramalısınız.

4 Birden fazla ve kolay erişim seçeneği barındırdığından emin olun

Doğru kilidi ararken sadece sizin için değil, aile bireyleriniz ve ziyaretçileriniz için de kullanımının kolay olup olmadığını önemseyin. Günümüzün akıllı kilitleri, kod girmek için dijital ve dokunmatik ekranlar, uzaktan kontrol cihazları, bir tıklamayla açılan telefon uygulamaları, parmak izi okuması ve geleneksel anahtar delikleri gibi özellikler sunar. Seçeceğiniz kilit de eve girmek ya da ev kapısını kilitlemek için birkaç farklı yol içermeli ve herkes kendisine en uygun olanı kullanabilmelidir.

5 Diğer akıllı cihaz ve uygulamalarla bağlantısını kontrol edin

Eğer diğer akıllı cihazlarınızla bağlantı kuramıyorsa akıllı kilidiniz gerçekten akıllı sayılamaz. Akıllı kilidinizin özellikle eviniz için kullandığınız diğer uygulamalarla bağlantı içinde olduğundan emin olun. Bu durum size evinize dair daha bütüncül bir koruma sağlar ve daha iyi bir yaşam tarzı sunar.

Akıllı kilit sistemlerinin uygulama desteği büyük kullanım avantajı getiriyor.

MUL-T-LOCK

DİJİTAL TAKSİ "TAXİ 7X24" İLE GÜVENLİ YOLCULUK

Dünyada ilk defa taksimetreyi içine alarak, mobil uygulamaları tablete uyarlayan Taxi 7x24 platformu, Turkcell'in güçlü 4.5G altyapısı ve uygulamalarını da kullanarak hem şoförler hem de müşterilere dijital yolculuğun keyfini yaşatacak. Platform sayesinde, Turkcell altyapısı ve uygulamalarıyla dijital hale gelecek taksiler, mobil Taxi 7x24 uygulamasının yanı sıra ilk defa BiP üzerinden çağrılabilecek.

Paycell ödeme alt yapısıyla da yolcular kredi kartı ile güvenli ödeme yapabilecek. Yeni nesil taksi yönetim platformu Taxi 7x24 kullanan araçların içinde şoförler ve yolcular için iki ayrı tablet bulunacak. Şoförler tablet üzerinden taksi çağrılarını görebilecek. Haritadan en iyi rotayı seçerek, taksimetrelerini takip edebilecek. Yolcular ise Turkcell'in dijital uygulamaları fizy, Dergilik, TV+ ile trafik derdini unutacak. Ayrıca yolcular sisteme entegre edilen alışveriş hizmetleri, haber ve eğlence içerikleriyle yolculuğun tadını çıkaracak. Böylece yolculuk sırasında Turkcell 4.5G ile tabletten internette gezinmenin keyfini yaşayacak

TAXİ 7×24 BİZLERE NELER SUNUYOR?

Hayatın her alanında yaşanan dijitalleşme, Turkcell'in altyapısını ve dijital uygulamalarını kullanan Taxi 7×24 platformuyla taksilere de geliyor. TETAŞ Elektronik'in taksi platformu Taxi 7×24, mobil iletişim, içerik ve ödeme altyapısı için Turkcell ile işbirliğine giderek taksileri dijital hale getiriyor. Dijital taksi, Taxi 7×24 ile taksiciler ve müşteriler daha güvenli ve konforlu yolculuk yapabilecek.

Tek merkezden kontrol edilebilecek taksilerin, hangi dakika nerede oldukları görülebilirken, dijital hale gelen taksimetreler de yine aynı merkezden sıra beklemeden kolayca uzaktan güncellenebilecek.

HEM ŞOFÖRE HEM YOLCUYA TABLET!

Sistem için her taksinin içine biri yolcu kullanımında olmak üzere iki adet tablet yerleştirilecek. Bu tabletler sayesinde şoförler, taksi çağrılarını kolayca alabilecek, gidecekleri yeri navigasyon üzerinden bulabilecek. Müşteriler ise tablet üzerinden internete girecek, kendilerine sunulan içeriklere göz atabilecekler.

TAXİ 7×24, TURKCELL SERVİLERİ İLE ENTEGRE OLACAK!

7×24 platformunda taksi çağırma ve ödeme sistemleri de yerli olacak. Sisteme entegre hale getirilen BiP uygulaması ile yolcular kendisine en yakın taksiyi tek dokunuşla çağırabilecekler. Yerli ödeme sistemi Paycell sayesinde de yolcular isterse taksi ücretini Turkcell hattı üzerinden ödeyebilecek ve bunu ay sonunda gelen faturasında görecek. Ayrıca kredi kartı üzerinden yapılacak ödemelerde de Paycell altyapısı kullanılacak.

TAKSİCİYE EK KAZANÇ SAĞLANACAK

Uygulama ile taksicilere daha fazla para kazanmanın yolu da açılıyor. Tablet içinde yer alacak reklam uygulamaları yolcular tarafından izlendikçe taksici daha çok kazanacak. Taksiciler bu uygulama sayesinde, yakın bir zamanda Turkcell Akademi üzerinden gerekli tüm eğitimleri de alabilecek. Yabancı dil, ilk yardım, şehir bilgisi gibi konularda eğitim alacaklar.

TURKCELL'DEN TAKSİCİLERE ÖZEL TARİFE

Taxi 7×24'ün aynı zamanda sürücülere de özel tarife sunacak. 4 GB ve 6 GB iki paket olarak sunulan tarifede 1000 dakika ve 100 SMS'in yanı sıra BiP, fizy, TV+, lifebox ve Dergilik dijital uygulamaları da yer alacak. Bu uygulamalar için de toplamda 16 GB'lık ek internet paketi tanımlanacak. Böylece ilk tarifeye seçenlerin paketlerinde toplam 20 GB internet yer alacak. İkinci tarifede ise bu rakam 22 GB'a çıkacak.

Kamera

Hava Koşullarına Dayanıklı Ev Güvenlik Kamerası: Circle 2

Rakiplerine göre bu modelin en büyük avantajı, zor koşullarla baş edebilmesi.

Klavye ve fareleriyle daha çok tanıdığımız Logitech, son yıllarda yeni nesil kamera ürünleriyle de sıklıkla karşımıza çıkıyor. Şirketin yeni ev güvenlik kamerası olan Circle 2, ev içinde ve dışında kullanım imkânı sunuyor.

Kablolu ve kablosuz iki seçeneği bulunan kamera, olumsuz hava koşullarına dayanıklı olarak geliştirilmiş. -20 derece soğukta veya 50 derece sıcakta bile sorunsuz kullanılabilen ürün; kapıya, prize, duvara, cama, arzu edilen her yere yerleştirilebiliyor.

Şarj edilebilir yedek pil seçeneğiyle uzun süre kesintisiz kullanılabilen Circle 2'ye, IOS ve Android akıllı cihazlar ve internet üzerinden de anlık olarak erişilebiliyor.

Yüksek kalitede görüntü alıyor

Evde olup biteni canlı ve HD kalitesinde görüntülemeye imkân tanıyan kamera, iki yönlü konuşma ve dinleme özelliği, 180 derece yüksek açılı lensi ve gece görüşü özellikleriyle dikkat çekiyor.

İnsanlar güvenlik problemleri için basit ve etkili bir çözüm arıyor. Circle 2, insanlara kameralarını nereye isterlerse oraya yerleştirme özgürlüğü vererek, evlerindeki herhangi bir güvenlik probleminden anında haberdar olmalarını sağlıyor.

Akıllı eve entegre olabiliyor

Circle 2, gelişmiş güvenlik ve kontrol için akıllı ev platformları ve aksesuarlarıyla uyumlu çalışıyor. Amazon Alexa ve

Logitech POP Akıllı Düğme'yle birlikte kullanılabilen kamera, kısa bir süre sonra Apple HomeKit ile de uyumlu çalışacak.

Logitech Circle Safe Premium aboneliğine sahip olan kullanıcılar, evde dolaşan insanların tespiti, evin belirli bölümlerinin izlenmesi, özel günler için talimat verilmesi ve verilerin uzun süre saklanması özelliklerinden yararlanabiliyor.

Logitech Circle Safe Basic aboneleri ise 14 günlük kaydedilmiş videolara ulaşma, uyarı hassasiyetini değiştirerek 15 veya 30 dakikaya ayarlama imkânını elde ediyor.

Metal yüzeylere tutturulabiliyor

Magnetic Mount sayesinde kablolu ya da kablosuz Circle 2, yağmur olukları, metal kapı çerçeveleri, çelik direkler ve aydınlatma armatürleri gibi manyetik yüzeylere kolayca takılabiliyor. Magnetic Mount'la gelen opsiyonel bir metal plaka ve yarı kalıcı bir yapışkanla birlikte, herhangi bir zemin montaj için uygun için manyetik bir yüzeye hızlıca dönüştürebiliyor. Hızlı ve kolay bir şekilde kurulabilen ürün, montaj için herhangi bir vida veya alete ihtiyaç duymamasıyla göze çarpıyor.

Apple HomeKit ile uyumlu

Circle 2 Kablolu Ev Güvenlik Kamerası, bir süredir Apple HomeKit ile uyumlu çalışıyor. Apple Home uygulaması sayesinde iPhone, iPad ve Apple Watch üzerinden ev anlık olarak izlenebiliyor, kilit ekranında bildirimler görülebiliyor.

Kamera tarafından evde bir hareket fark edildiğinde HomeKit ışıkların yanmasını sağlıyor ayrıca istenmeyen ziyaretçileri uzak tutmak için bildirim ayarlamaları yapılabiliyor. Siri komutlarıyla uygulama üzerinden kolayca yönetilebilen kamera, Circle 2 Companion iOS uygulaması Logi Circle'ı kullanılarak günlük bilgilendirme gibi gelişmiş özellikler sunuyor.

SHIELD.COM.TR

SORU-CEVAP
Temassız Ödeme

SORU: Son yıllarda yaygınlaşan temassız kredi kartı ve banka kartı kullanımında herhangi bir güvenlik sorunu var mı? Temassız ödeme güvenli midir? Benden izinsiz para çekimi yapabilirler mi?

Öncelikle temassız ödemenin ne olduğunu kısaca açıklayalım. Temassız Ödeme, hızlı, kolay ve güvenli bir şekilde işlem yapmanız için geliştirilmiş bir teknolojidir.

Temassız kartınızı, temassız okuyucusu olan noktalara yaklaştırarak ödeme işlemlerinizi yapabilirsiniz. 1 saniyeden kısa sürede onaylanan temassız ödeme işlemleri, kartın üzerinde yer alan çipe bağlı olan anten ve POS üzerinde yer alan okuyucunun radyo frekansı dalgaları üzerinden haberleşmesiyle gerçekleşir. Temassız teknolojisi ayrıca, NFC özellikli cihazlar ile POS'larda ödeme yapabilmeyi mümkün kılar.

Şimdi asıl sorumuza gelelim: Temasasız ödeme güvenli mi? Kesinlikle! Temassız özellikli kart ve cihazlar, ulusal ödeme şemalarının getirdiği güvenlik standartlarına tabi. Ayrıca ödeme kabul cihazları, bankaların belirlediği risk kriterlerine uygun kişilere veriliyor ve bankaların devamlı kayıt ve takibi altında bulunuyor.

Temassız ödemeler, kartın elden bırakılmamasına imkân sağladığı için kaybolma, çalınma ve kopyalanma riskini azaltıyor. Temassız ödemeler ayrıca kasa yönetiminde nakit operasyonunun getirdiği hata, sahte para, nakit para taşıma ve nakit parayı koruma maliyeti konularında da avantaj yaratıyor.

Medyada dönem dönem hortlatılan "mobil posla dışarıda temassız kartlardan izinsiz para çekilmesi" haberlerini de ciddiye almayın. Temassız işlemlerde ödemeyi kabul etmeye hazır olan okuyucu cihaza en fazla 4 santimetre mesafede olmak gerekiyor; bu sebeple bilginiz dışında temassız işlem yapılması olası değil.

Banka ve kredi kartınızda temassız ödeme seçeneği varsa güvenle kullanabilir; yoksa bankanızdan temassız destekli kartınızı isteyebilirsiniz.

Mağazalar Akıllı Kameralarla Daha Güvenli

Üzerindeki yazılımlar sayesinde şüpheli bir durumu anında fark ederek, operatörü uyaran yeni nesil güvenlik sistemleri, hem kayıpları, hem de güvenlik maliyetlerini azaltıyor.

Hâlihazırda kullanılan güvenlik kameraları sadece kayıt yapıyor ve operatörler bu kayıtların sadece yüzde 4'ünü izleyebiliyor. Sektörün lider elektronik güvenlik sistemleri entegratörü Sensormatic'in sunduğu Uzaktan İzleme Çözümleri ile ise hiç bir ayrıntı gözden kaçmıyor.

Kameralar üzerlerindeki akıllı yazılımlar sayesinde izinsiz giriş, şüpheli bir paket ya da boş dolaşan biri anında fark edilerek Uzaktan İzleme Merkezi'ne ulaştırılıyor, operatörler gerekli önlemi anında alıyor. Erken uyarı ile pek çok olay daha gerçekleşmeden önleniyor.

Uzaktan izleme çözümlerinde yeni nesil elektronik güvenlik teknolojileri, güvenlik elemanları ile harmanlanıyor, güvenlik bir üst seviyeye taşınıyor. Maliyetlerde de önemli tasarruf sağlanıyor. Mevcut sistemlere entegre edilen sistemlerin kurulumu son derece hızlı gerçekleşiyor. Ayrıca perakendeciye herhangi bir yatırım ya da operasyonel yük gelmiyor. Sistem yönetimi ile uçtan uca bir hizmet olarak sunuluyor.

Sistemin Kullanım Alanları

Uzaktan alarm doğrulama: Uzaktan İzleme Merkezi'ne gelen bir alarmın gerçekliğini, mevcut kamera sistemine uzaktan bağlanarak doğrulamak mümkün. Bu durum, güvenlik görevlilerinin yanlış alarmlara müdahale etmelerini engellerken, uzaktan anons imkanı ile suç gerçekleşmeden suçluyu caydırma imkanı veriyor.

AYLAK DOLAŞAN KİŞİ: Özellikle büyük mağazalarda sık rastlanan, belli bir bölgede amaçsız dolaşan kişiler sistemle fark edilerek, izlemeye alınıyor. Bu şekilde mağaza içi kayıp oranları azalıyor.

SANAL DEVRİYE: Mağazanın ya da deponun kamera sistemlerine internet üzerinden erişerek, devriye hizmetini uzaktan gerçekleştirmek mümkün. Bu durum, özellikle güvenlik zaafiyeti olan yerlerin daha az riskle korunmasını sağlıyor.

ÇEVRE KORUMA: Mağazaların çevresine veya giriş noktalarına kurulan akıllı kamera sistemleri de alarm sistemi gibi hareket edebiliyor. Herhangi bir ihlal anında (izinsiz bir bölgeye giriş, uzun süreli bekleme, gibi) ilgili alarm görüntüsü Uzaktan İzleme Merkezine ulaşıyor ve operatörler tarafından etkili ve erken müdahale imkanı yaratılmış oluyor.

YOĞUNLUK TESPİTİ: Belli bir bölgede, kalabalığın sıra dışı şekilde toplandığı fark edildiğinde sistem, bu uyarıyı merkezi iletiyor. Yoğunluk tespiti, mağazalarda yada süpermarketlerde yeni kasa açmak ihtiyacını önceden haber vermek açısından da kullanılabiliyor.

UZAKTAN GİRİŞ-ÇIKIŞ YÖNETİMİ: Mağazaya yapılan giriş-çıkışlar Uzaktan İzleme Merkezi'ndeki operatörler tarafından uzaktan yönetilebiliyor. Kullanılan geçiş kontrol ve kamera sistemleri ile daha az insan gücü ile daha ekonomik ve etkili çözüm imkânları yaratmak mümkün.

Ev Güvenlik Sistemi Satın Alırken Bunlara Dikkat Edin!

Kendimizi en güvende hissettiğimiz yer evimizdir. Bunu korumak için teknolojiden faydalanın.

Çağımızın en büyük problemlerinden biri olan güvenlik, insanların hem sağlığına hem de doğrudan sahip olduğu maddi birikimlerini etkisi altına alıyor. Birçok ev ve iş yerinde gördüğümüz elektronik güvenlik sistemleri sayesinde, hırsızlık ve diğer tehditler büyük oranda engellenebiliyor. Siz de bu konuda satın almalara gitmeyi düşünüyorsanız bu rehber epeyce işinize yarayacak.

Kamera ve alarm sistemleri sayesinde, yaşam alanlarımızı daha güvenilir hale getirebiliriz. Üstelik öyle büyük yatırımlar da gerekmiyor. Alışveriş sitelerindeki ev güvenlik sistemleri bölümünde ev ve işyeri güvenliğinizi sağlamak adına alarm ve kamera çözümlerini bulabilirsiniz. Bu alanda seçim yapmak ise tamamen düşüncelerinize kalmış durumda. İş yerinizin dış görünümü, içerisindeki dizilim ve aynı şekilde evinizin iç dizaynı gibi kriterler, nasıl bir güvenlik sistemi kurmanız gerektiğine işaret edebilir. Rehber içerisinde de bu konu üzerinden ilerleyeceğiz. Alarm ve güvenlik sistemleri sanıldığından çok daha geniş bir alanı kapsıyor. O nedenle bazı bölümleri satır satır açıklıyoruz.

İdeal güvenlik sistemi için satın alma ipuçları

Sahip olmanız gereken güvenlik sistemi için öncelik ve tercihlerinizi belirlemelisiniz.

1 Gizlenmiş küre kameraları tercih edebilirsiniz

İş yerinizin bir vitrini mi var? Cam kırılmalarına ve çatlamalarına karşı hassas sensörlere sahip alarm sistemlerini tercih edebilirsiniz. Bir giyim mağazanız var ve mağazanın bazı alanları görüş açınızın dışında mı kalıyor? Bunun için Dome olarak adlandırılan ve ufak küre şeklinde kameraları tercih edebilirsiniz. Bu kameraların, insanlar tarafından fark edilmesi kolay değil. Çünkü aynı yangın söndürücüsünü andırıyorlar.

2 Uzaktan erişilen kameralar harika

Çok seyahat ediyor ve iş yerinizi uzaktan izlemek mi istiyorsunuz? Ayrıca çalışanlarınızın da neler yaptığını görmek, içinizi rahatlatırdı değil mi? İhtiyacınız olan şey kesinlikle IP kameralar! Saniyede 30 kare oranı sağlayabilen bu kameralara, internetin olduğu herhangi bir yerden kolayca ulaşabilirsiniz. Ayrıca özel bir yazılım ile sayesinde, izlediğiniz görüntüleri bilgisayarınıza da kayıt edebilme imkânınız bulunuyor.

3 Dijital kayıt yapan sistem işinizi kolaylaştırır

DVR kartı alarak onu PC'nize bağlamayı mı düşünüyorsunuz? DVR kartını taktığınız PC'nin donanımsal kaynakları taktığınız DVR kartına aktarılacak. Yani PC'nizi kullanmakta güçlük yaşayacaksınız. Fakat DVR konusunda ısrarlıysanız, kendi içerisinde dijital kayıt mekanizması bulunan ürünleri tercih edebilirsiniz. Tabii küçük ölçekli bir işyerini işletiyorsanız, böyle bir mekanizmaya da ihtiyacınız yok.

4 Birden fazla kamera için özel çözüm

Ev veya işyerinize birden fazla kamera koymak ve hepsini tek ekran üzerinden kontrol etmek mi istiyorsunuz? Bu isteğinizi gerçekleştirmeye yönelik hazırlanmış olan Multiplexer cihazlar sayesinde, isteğinizi gerçekleştirebilirsiniz. Aynı zamanda Multiplexer kullanarak, görüntüyü 1'den fazla ekrana da aynı anda yansıtabilirsiniz. Multiplexer özelliğini DVR kayıt cihazlarında görebilirsiniz.

5 DVR çözümünün türüne karar verin?

Hardware DVR ve Software DVR arasında mı kaldınız? Hardware DVR kartların kendi merkezi işlemcileri ve fiziksel bellekleri bulunuyor. Böylece bilgisayarın işlemcisine yük bindirmeden işlemlerini gerçekleştirebilir. Software DVR ise tüm kaydetme ve oynatma gibi işlemleri, bağlı olduğu bilgisayarın kaynaklarından yararlanarak gerçekleştiriyor. Bu durumda bilgisayarı kullanmanız oldukça zorlaşıyor.

6 Nedir bu FPS sayısı?

Neden bazı DVR kart modellerinde 50 FPS, bazılarında ise 200 FPS yazıyor? Bir DVR kartı aldınız ve saniyede 50 kare oranına sahip. TV'de izlediğiniz filmlerin saniyede gösterdiği kare sayısı 25. Sinemada izlediğiniz filmlerin ise 24. Yani insan gözü 24-25 FPS'te akıcı görüntüler elde edebiliyor. DVR cihazınıza bağlamak istediğiniz bir kameradan akıcı görüntüler elde edebilmeniz için 25 FPS yeterli olacaktır.

Çocuğunuzu YouTube'daki Tehlikelerden Koruyun!

Popüler video platformu YouTube, çocuklar için faydası kadar tehlikeyi de barındırıyor.

Çocuğunuzun sadece YouTube'da değil, genel olarak internette daha güvende olması için baskıcı olmadan tedbirli olmayı başarmalısınız.

YouTube çocuklar için uzun vakitler geçirebilecekleri eğlenceli bir ortam olabilir ama bu, çocuklarınızı YouTube'la baş başa bırakıp rahatça başka şeylere dalabileceğiniz anlamına gelmiyor. YouTube'da çocuklar için zararlı içerikleri, devasa sayıda katkı yapan kullanıcılar göz önüne alındığında, tamamen engellemek zor olabilir. Yine de güvenliği içeriği artırmak mümkün.

Kısıtlı içeriği etkinleştirin

YouTube'da zararlı içerik engellemenin en kolay yolu "Kısıtlı Mod"u açmak. Ana sayfanın en altından açılıp kapatılabilen Kısıtlı Mod'un (YouTube'un ayrıntılı yardım sayfası) nerede işe yarayıp nerede işe yaramadığına değinelim.

Kullanıcı bildirimleri etkili

YouTube'a göre Kısıtlı Mod, diğer kullanıcıların bildirimlerine göre oluşuyor ve yaş kısıtlaması ya da uygun olmayan içerik bu bildirimlere göre belirleniyor. Diğer bir deyişle, videoların çocuğunuza uygunluğu sadece sade vatandaşın uygun görüp görmemesine ve Google'ın algoritmalarının insafına bırakılıyor. YouTube bu yöntemin %100 güvenilir olmadığını en baştan söylüyor. Bu kısıtlamaları atlatmak da basit. Ana sayfanızda çocuk videolarının yanında uygunsuz videolar belirmiyor olabilir ama Kısıtlı Mod, arama işlevini tamamen ortadan kaldırmıyor ve içeriğinde müstehcen konuşmaların veya uygunsuz şakaların yer aldığı arama sonuçları göstermeye devam ediyor. Fakat örneğin Call of Duty araması yapıldığında, bu oyun 18 yaşından büyükler için sınıflandırıldığı için birçok sonuca ulaşılamıyor.

Kısıtlı mod filtresi her yerde çalışmıyor

Kısıtlı Mod'un işe yaradığı videolar arasında çocuklarca oldukça popüler olan Minecraft videoları var. Çocuklara özel Minecraft kanalları arasında en popüler olanlarından Stampy'de küfürden özellikle kaçınıldığını görebiliyoruz. Buna karşın Yogscast adlı ağırlıklı olan Minecraft üzerine olan diğer bir YouTube kanalında ise küfür ve erişkin içerik engellenmezken, Kısıtlı Mod etkinleştirildiğinde bu kanalın hâlâ erişilebilir olduğunu görüyoruz. Kısıtlı Mod'un bir diğer açığı da ülkemizde olmasa bile yurtdışındayken alkol reklamlarını göstermeye devam etmesi.

Tarayıcıda özelliği kilitleyin

Kısıtlı Mod'u web tarayıcınızda etkinleştirir etkinleştirmez YouTube size mevcut tarayıcınızda bu özelliği kilitlemenizi de öneriyor ki bizim de tavsiyemiz bu yönde. Bu sayede siz kendi hesabınızdan çıkış yapsanız bile aynı tarayıcıdan YouTube'a başka bir hesapla girildiğinde Kısıtlı Mod etkin kalıyor. Tabii çocuğunuz yeterince kurnazsa tarayıcının gizli gezinti moduna geçerek veya farklı bir tarayıcı kullanarak bu engeli aşabilir. Kısacası hiçbir önlem çocuğunuza bizzat nezaret etmenizden daha etkili değil.

"Kanallara göz at" sayfasında "çocuk" araması yapınca çocuklara yönelik birçok kanal çıkıyor.

Nereden başlamak gerekiyor?

Ülkemizde YouTube kanallarına gösterilen ilgi ABD'deki eşdeğerlerine göre biraz kısıtlı. Türkçe içerikli kanal bolluğu azımsanmayacak ölçüde olsa en fazla abonesi olan TRT Çocuk'un üye sayısı 71 binlerde, fakat kanala video yüklenme sıklığı çok iç açıcı değil.

“Çocuğunuz ne tür videolar izliyor? Yabancılarla etkileşim kuruyor mu? Gördüğü içerikler yaşına uygun mu?”

“Kanallara göz at” düğmesinden “çocuk” yazarak ulaştığımız kanallar arasında eğitici olanları da bulunuyor. Ayrıca bolca oyuncak tanıtımına rastladık.

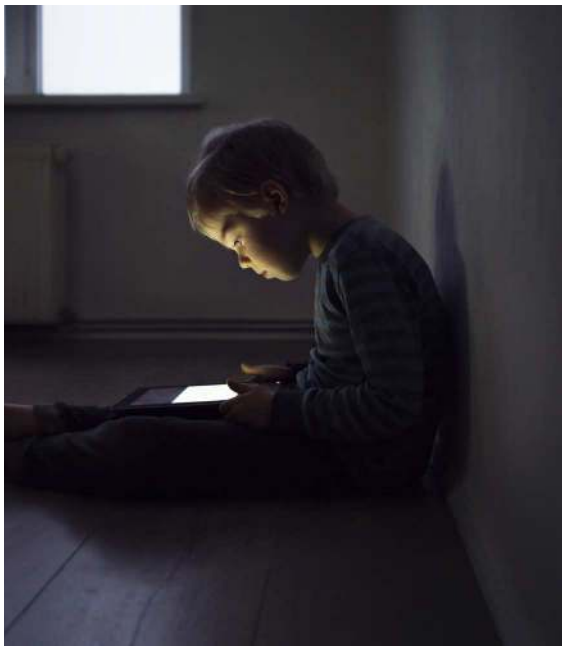
Eğer çocuğunuza İngilizce içerik izletmek istiyorsanız yaş gruplarına göre YouTube kanalları öneren Common Sense Media’nın sitesine (bitly.com/cocuk221) göz atabilirsiniz.

YouTube büyük bir pazar

YouTube için çocuklara yönelik içerik pazarı tahmin edebileceğimizden çok daha büyük. Sadece geçen yılın eylül ayında YouTube’daki en popüler 10 kanaldan 5’ini çocuklara yönelik kanallar oluşturuyordu ki bunlar arasında oyuncak testleri, çizgi filmler, şarkılar ve video blogları (Dünyanın En Çok Görüntülenilen 50 YouTube Kanalı) geliyor. Çocuk içeriği olmayan geriye kalan 5 kanaldan 3’ü müzik, (biri Türkçe netd), biri Amerikan güreşi ve sonuncusu da Amerikan internet medya devi Buzzfeed’in kanalları.

YouTube bu verileri göz ardı etmemiş olacak ki 2015’in Şubat ayında Android ve iOS cihazlara yönelik YouTube Kids adlı bir uygulama çıkardı. Çocuklara yönelik her şeyin güvenle aranıp bulunabildiği bu uygulama sadece Amerikan App Store’dan indirilebiliyor fakat uygulamanın masum olmadığını düşünenler de var. Daha ilk aylarında ABD Federal Ticaret Komisyonu tarafından gözlem altına alınan uygulama; McDonald’s ve Lego gibi firmaların kanallarının öne çıkarılması, diğer birçok firmanın da oyuncak testleri videolarında ürün yerleştirme yapmasını sorguluyor.

Aslında bu yeni bir şey değil. ABD’de çizgi filmlerin içine gizlenmiş marka reklamları on yıllardır süregeliyor, fakat artık çok daha bilgili ve birçok konuya şüpheci yaklaşan ebeveynler sayesinde YouTube daha dikkatli olmak zorunda. Uygulama bir gün Türkiye App Store’una gelirse süre limiti, ses düzeyi sınırlayıcı, arama fonksiyonunu kapama ve sadece uygulama tarafından önerilen videoları seyredebilme özellikleriyle çocuklarımızı baş başa bırakma lüksüne sahip olacağız. ●



Çocukların Güvenli Sosyal Ağ Kullanımı İçin Ebeveynler Hangi Önlemleri Almalı

Çocukların çoğunlukla dışarıda oynadığı ve sadece acıktıklarında eve geldikleri zamanlar geride kaldı. Günümüzde dışarı çıkmak yerine günde birkaç saatlerini internette, sosyal ağların sanal gerçekliğinde harcıyorlar. Teknoloji çağında yaşayıp teknoloji ile tanışmadan yaşamalarını istemek olası görünmüyor. Ancak sosyal ağ kullanımını daha güvenli hale getirmek mümkün.

ÇOCUKLARINIZLA KONUŞUN

Diyalog, özellikle konu sosyal ağlar olduğunda, çocuklarınızı çevrimiçi ortamda güvende tutmanın en önemli unsurlarından biridir. Çocuklarınızın kararınıza güvenmesini ve tavsiyelerinize uymasını istiyorsanız, kanalları ve zihninizi sorulara ve tartışmaya açık tutmak çok önemlidir. Siber zorbalık ve bunun önlenmesi buna iyi bir örnektir. Kızınıza veya oğlunuza, bu tür bir davranışla karşılaştıkları takdirde doğrudan onları ilgilendirmese bile (nerede olduğuna bağlı olarak) size, öğretmenine veya eğitmenine hemen haber vermeleri gerektiğini açıkça belirtin. Elinizdeki tek kanıt olduğundan zorbalık mesajını sakın silmeyin.

Güncel bir güvenlik çözümü tercih edin

Kötü amaçlı yazılımlar siber dünyadaki en yaygın tehditlerden biri olduğundan, sosyal ağları kullanırken virüslerden kaçınmak için proaktif algılama yeteneklerine sahip bir virüsten korunma yazılımı ve çocuğunuzun cihazlarına güncel bir imza veritabanı kurmak gerekir. İstenmeyen e-postaları engelleme ve güvenlik duvarı araçları da bu riskler karşısında sistem güvenliği optimizasyonunu mümkün kılar. Ayrıca çocuğunuz sosyal ağlarda gezinirken asla bir yönetici hesabı kullanmamalıdır. Güvenlik sorunlarının etkisini en aza indirmek için çocuklarınız için özel bir kullanıcı profili oluşturabilirsiniz.

EBEVEYN KONTROLÜ YAZILIMI KULLANIN

Çocuklarınızın yaşına bağlı olarak ebeveyn kontrolü yazılımından ve özelliklerinden yararlanabilirsiniz. Böyle bir yazılım içeren ESET Internet Security, engelleyeceğiniz web sitelerinin listesini oluşturmanıza ve ayrıca çocuğunuzun çevrimiçi olarak harcayabileceği zaman ve saat miktarını kısıtlamanıza olanak tanır. Diğer yandan, çocuklar da söz hakkına sahip olmalıdır. Telefon ve tabletlere yönelik ebeveyn kontrolü yazılımı ESET Parental Control for Android, çocukların belirli bir web sitesini ziyaret etmek veya sosyal ağda geçirdiği süreyi uzatmak için izin istemelerine olanak sağlar.

PAROLANIZ GÜÇLÜ OLSUN

Güvenli bir parolanın nasıl olduğunu çocuklarınız biliyor mu? "Parola" veya "12345" gibi tahmin edilmesi kolay seçenekleri kullanmadıklarından emin olun. Ayrıca şifre en az 10 karakter uzunluğunda olmalı, büyük ve küçük harf, sayı ve # veya @ gibi özel bir sembol içermelidir. Parolalarını hiç kimseye, hatta en iyi arkadaşlarına bile vermemelerini hatırlatmayı da unutmayın.

İKİ FAKTÖRLÜ DOĞRULAMAYI KULLANIN

Çocuklarınızın Facebook, Twitter veya diğer popüler sosyal ağlara bağlanırken güvenlik ayarlarında sunulan iki faktörlü doğrulamayı kullanmasını sağlayın. Akıllı telefonlarına tek kullanımlık bir parola gelmesi, saldırganlar için kırması zor olan başka bir güvenlik katmanı ekler.

SOSYAL AĞLARDA DOĞRU GİZLİLİK AYARLARINI KURUN

Varsayılan sosyal ağ gizlilik ayarları, çocuğunuzun güvenliğini garanti etmez. Bu nedenle ayarları doğru bir şekilde yaparken yeterli zaman ayırmanız ve hangi

Çocuklarınızın sosyal medya merakını yasak koyarak değil, tedbir alarak yönetebilirsiniz.

bilgilerin sızabileceğini kontrol etmeniz önerilir. Örneğin Facebook'ta çocuğunuzun profilindeki hiçbir profil ayarının istisnasız herkese açık olmadığından emin olun. Tercihen, bilgileri sadece arkadaşlarına, eğer arkadaşları çok fazla ise sadece küçük bir gruba (aile veya yakın arkadaş gibi) erişilebilir hale getirin. Çocuğunuzun etiketlendiği resim, durum ve diğer içerikleri görebilecek kişileri sınırlayın. Uygulamaların kendi kişisel bilgilerine erişmesini veya duvarlarında gönderim yapmasını engelleyin. Sadece kişisel olarak tanıdıkları insanlardan gelen arkadaşlık tekliflerini kabul etmelerini öğretin. Ayrıca siber dünyada yabancılarla konuşmanın veya iletişim kurmanın, gerçek dünyada olduğu kadar tehlikeli olabileceğini belirtin.

ÇOCUKLARINIZLA ONLİNE VAKİT GEÇİRİN

Çevrimiçi olarak çocuklarınızla vakit geçirin ve bu şekilde onların en sevdiği web adreslerini görebilme imkanını elde edin. Çocuklarınıza, yaşlarına uygun sosyal ağları kullanmalarını tavsiye edin. Zor olacaktır ama acil durumlar için e-postalarına veya diğer hesaplarına erişebilme hakkını isteyin.

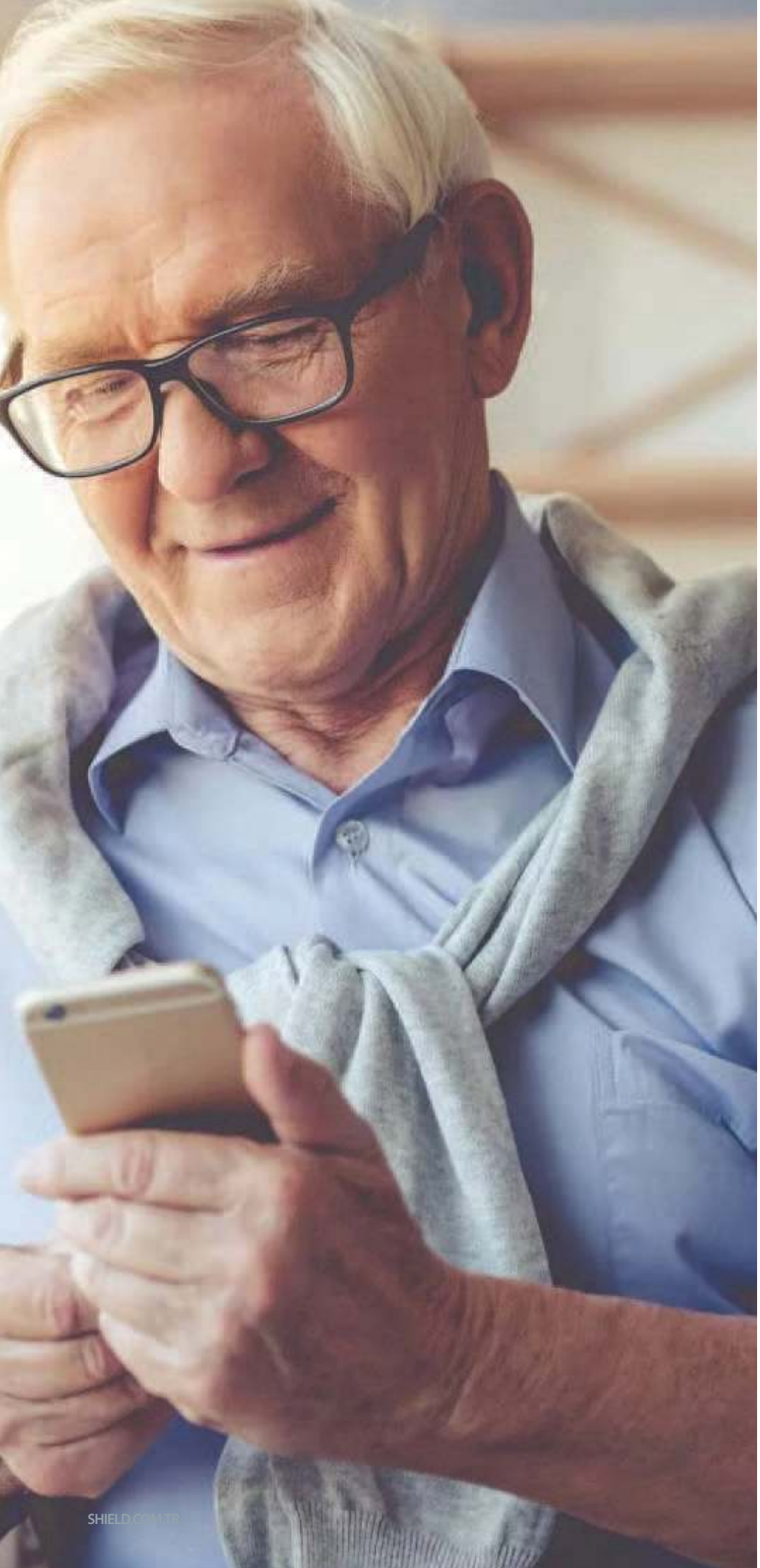
YAŞLILAR İÇİN MOBİL GÜVENLİK SORUNU BÜYÜYOR

KÖTÜ NİYETLİ İNSANLAR VE DOLANDIRICILAR İÇİN KOLAY KANDIRILAN VE TEKNOLOJİYE MESAFELİ OLAN YAŞLILAR EN RAHAT AV OLUYOR.

Gerçekleştirilen "Mobil Tüketici Anketi"ndeki verilere göre 55 yaş ve üstü tüketicilerin akıllı telefon kullanım oranları, gençleri yakaladı. 55 yaş ve üstü ABD'li tüketiciler, mobil cihaz ve hizmetlerin benimsenmesi ve kullanılmasında ön sıralarda yer almaya başladı. Bununla birlikte, siber suçluların ağına daha kolay düşen yaşlı insanlar, mobil cihazlarla birlikte daha erişilebilir hale gelmiş oldu.

Deloitte'un 2017 Küresel Mobil Tüketici Anketi'nin ABD'ye yönelik araştırmasından ilgi çekici sonuçlar ortaya çıktı. Teknolojideki eğilimleri göstermesi açısından önem taşıyan araştırmaya göre 55-75 yaş grubu kategorisi, akıllı telefona sahip olma oranında son iki yılın en yüksek büyüme artışını sergiliyor.

Bu yaş grubundaki akıllı telefon kullanım büyüme oranı, üç yıllık ortalama büyüme göstergelerine göre yüzde 7,91 seviyesine ulaştı. 45-54 yaş arasındaki tüketiciler yüzde 7,88'lik büyüme oranıyla çok az geride. Belli bir doygunluğun gözlemlendiği 18-24 yaş grubundakilerde büyüme oranı sadece yüzde 1,40 düzeyinde. Tüm yaş gruplarında akıllı telefona sahip olma oranındaki toplam büyüme ise yüzde 5,42'ye ulaştı.



NEREDEYSE HERKESİN BİR TELEFONU VAR

En genç nüfusun yüzde 93'ü ve en yaşlı nüfusun yüzde 67'si artık bir akıllı telefona sahip. Toplama bakıldığında 18-75 yaşları arasındaki Amerikalıların yüzde 82'si bir akıllı telefona sahip ya da dilediği zaman akıllı telefon kullanabiliyor. Bununla birlikte, tablet kullanım oranı dört yıl öncesinde yüzde 31 iken, bu oran ikiye katlanmış durumda.

GÜNDE KAÇ KEZ TELEFONA BAKILIYOR?

Genel olarak, Amerikalıların son üç yılda cep telefonlarını günde ortalama 47 kez kontrol ettikleri tespit edildi. Burada ortalamayı yükselten 18-24 yaş grubu oldu. Bu grup, günde 86 defa (geçen yıl 82 idi) telefonunu kontrol ediyor. Anketin belirttiğine göre 'ABD'li 264 milyon akıllı telefon kullanıcısının tümü, bir günde toplam 12 milyar kez telefonlarına bakıyor!' Kullanıcıların yüzde 89'u uyandıktan sonra bir saat içerisinde telefonlarına bakarken, yüzde 81'i de uyumadan önceki bir saat içerisinde bu işlemi gerçekleştiriyor.

FAZLA MI KULLANIYORUZ?

34 yaşına kadar olan kullanıcıların yaklaşık dörtte üçü, telefonlarını 'kesinlikle' veya 'muhtemelen' çok fazla kullandıklarını dile getiriyor. Her yaştan kullanıcıların neredeyse yarısı (yüzde 47), cep telefonlarıyla geçirdikleri zamanı azaltmak amacıyla cihazlarını çantalarına veya ceplerine koyarak ya da bildirimleri kapatarak bilinçli bir çaba gösterdiklerini söylüyor.

ESKİ ALIŞKANLIKLARIN YERİNİ YENİLERİ ALIYOR

Anket, tüketicilerin yaklaşık üçte ikisinin akıllı telefonlarını iki yıl içinde yükseltmeyi hedeflediklerini ortaya koyuyor. Deloitte, mevcut sözleşmelerden feragat edilmesine değinirken, operatörlerin kiralama ve satın alma programları için yeni cihazlara duyulan sürekli ihtiyacı tazeleyerek oluşturulan 'ultra ilişkili toplum' taleplerini karşılamayı hedeflediklerinin altını çiziyor. Yalnızca değişim için yapılan alışverişlerin yanı sıra, tüketicilerin artan bir kısmı, eski cep telefonunu atmak yerine bir aile üyesine veya bir arkadaşa vererek alternatif çözümler üretebiliyor.

IOT İLE BİRLİKTE GÜVENLİK ENDİŞESİ ARTIYOR

Deloitte, önceki yılların bulgularıyla benzer bir şekilde, internetle bağlantılı nesnelerin tüketici özgürlüğünü ve ilgisini arttırdığını gözlemledi. Bununla birlikte,

insanların önemli bir bölümü IoT cihazların risklerinin farkında olmalarına rağmen, başlarına bir şey gelmeden harekete geçmiyor.

Araştırmada yer alan tüketicilerin yüzde 40'ından fazlası, akıllı ev teknolojisinin kişisel yaşamlarıyla ilgili çok fazla bilgi açığa çıkardığını ve yüzde 40'a yakın bir kısmı da kullanımın takip edilebildiğini düşünüyor.

Bu görüş, Accenture tarafından gerçekleştirilen bir araştırmada ortaya çıkan bulgularla da örtüşüyor. Araştırmaya göre, 'Tüketicilerin beşte birinden azı, akıllı ev cihazlarıyla ilgili güvenlik riskleri hakkında çok iyi bilgilendirildiğine inandığı ve yaklaşık yüzde 40'lık kesimin ise doğru bilgilendirilmediğini düşündüğü' belirtiliyor.

ENDİŞEYE RAĞMEN, TÜKETİCİLER CESUR DAVRANMAYI SÜRDÜRÜYOR

Gizliliğe ve güvenliğe bağlı kalma ihtiyacının farkında olmaksızın ankete katılanların yüzde 91'inin 'uygulamaları yüklemeden önce yasal koşulları okumadan kabul etmekte, Wi-Fi erişim noktalarını kaydetmekte, güncellemeleri kabul etmekte ve video akışı gibi çevrimiçi hizmetlere üye olmakta' olduğu ifade edildi.Deloitte, en genç iki grupta bu kabul oranının yüzde 97'ye çıktığını belirtti.

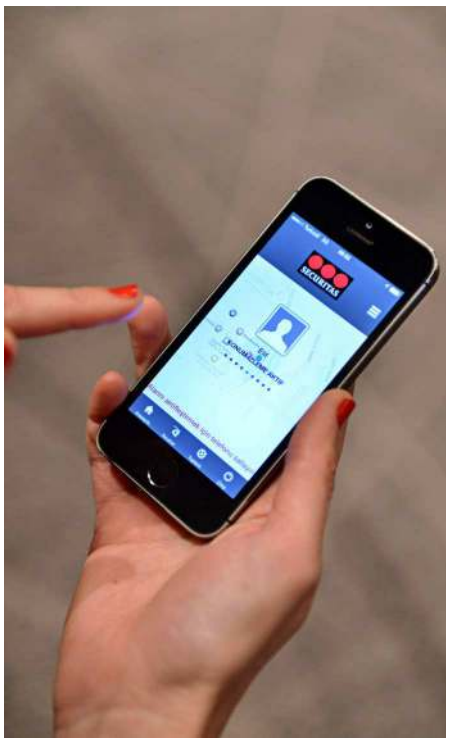
Gizlilik ve güvenlikle ilgili risklerin ortaya çıktığı ekran başında geçirilen uzun süreler, pek çok tüketici için yeni teknoloji ve hizmetlerin tehlikeli sularına dalmamak adına yeterli bir sebep değil.

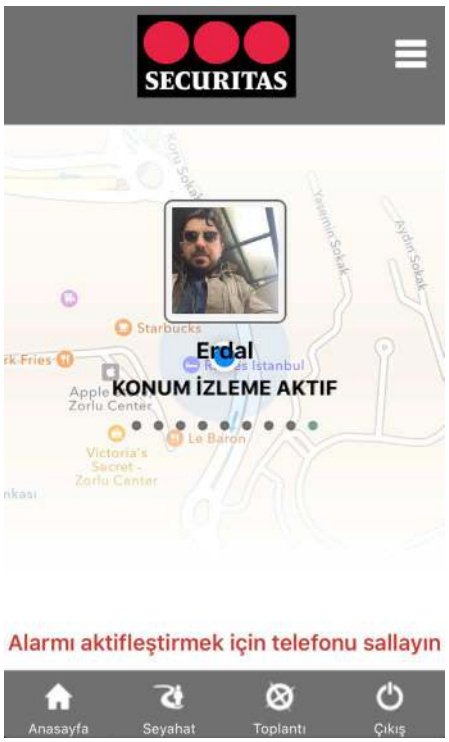
ABD'deki mobil dünyayı hedef alan ve bu yıl yedincisi yapılan araştırma, 18-75 yaş aralığındaki altı farklı yaş grubunda yer alan 2 bin katılımcıdan toplanan veriler doğrultusunda oluşturuldu.

GÜVENLİK HER YAŞTA LAZIM

İleri yaştakilerin teknolojiye entegre olmasını olumlu yorumlayan ESET Kıdemli Güvenlik Araştırmacısı David Harley, buna karşın güvenliğe dikkat edilmesi gerektiği uyarısında bulundu. Harley, "Siber saldırılar yaşlı veya genç tanımaz. Cihaz ya da uygulamadaki açıkları tanır. O nedenle tüketiciler, kullandıkları cihazlar hakkında bir miktar bilgi sahibi olmaya çalışmalı ve cihazın korunmasına yönelik güncel bir güvenlik yazılımı değerlendirmeli" diye konuştu.

> "Kaç yaşında olursa olsun herkesin teknolojinin nimetlerinden faydalanması bir insan hakkı."





Kişisel Güvenliğiniz İçin Mobil Uygulama:
Securitas Güvendeyim

Securitas Güvendeyim uygulaması ile acil durumlarda yerinizi bildirip hızlıca yardım alabilirsiniz.

İnsanların gündelik hayatlarında karşılaşabilecekleri güvenlik risklerini çözmek amacıyla tasarlanan "Securitas Güvendeyim" uygulaması ile genç-yaşlı, kadın-erkek herkes kendi güvenlik hizmetine sahip olabiliyor.

Özellikle metropol il ve ilçelerdeki insanların karşılaştıkları suçlara yönelik basit ve etkili bir mobil uygulama tasarlandı. Ağırlıkla kurum ve kuruluşlara entegre güvenlik çözümleri sunan Securitas, kişisel güvenliği sağlamak üzere, bireylerin rahatlıkla yararlanabilecekleri "Securitas Güvendeyim" uygulamasını kullanıma sundu.

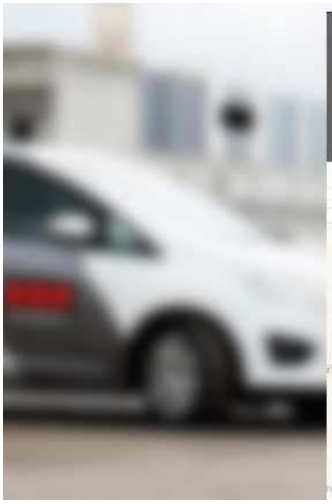
Bu uygulamayı akıllı telefonlarına indiren kullanıcılar, kişisel güvenliklerini tehdit edebilecek herhangi bir risk ile karşılaşmadan önce ya da karşılaştıkları an, sadece telefonu hafifçe sallayarak uygulamayı aktif hale getiriyor ve Securitas Uzaktan İzleme Merkezi'ne alarm iletebiliyorlar. İkinci kez telefonu sallamaları halinde, uygulamanın ışıklı alarm sesi özelliği harekete geçiyor.

SES VE GÖRÜNTÜ KAYDI İLE KONUM GÖNDERİYOR

Alarm ile birlikte, ses ve görüntü kaydı ile birlikte kullanıcının konum bilgisi de Merkez'e iletiliyor. Uzaktan İzleme Merkezi, alarm durumunda merkeze ulaşan bu bilgileri kullanarak kullanıcıya gereken yardımın mümkün olan en kısa sürede ulaşması için gerekli yerlere ve kullanıcı tarafından belirlenen kişilere bildirimde bulunuyor.

Akıllı telefonlarda kullanılan "Securitas Güvendeyim" uygulaması telefonla veya web sitesi üzerinden gerçekleştirilen abonelik ile aktifleştiriliyor. Uygulama ücretsiz indiriliyor ve yıllık abonelik sistemi üzerinden kullanılıyor. Abonelik işlemleri sırasında oluşturulan şifre ile kullanıcılar akıllı telefonlarına indirdikleri uygulamaya istedikleri zaman giriş yapabiliyorlar.

Securitas Güvendeyim uygulaması; geç saatte mesai çıkışında, şehir içi veya şehirlerarası seyahatlerde ve daha birçok risk durumunda, kullanıcılarına daha güvenli bir hayat sunuyor. Detaylı bilgi için ve indirme bağlantıları için **http://guvendeyim.securitas.com.tr** adresini ziyaret edebilirsiniz.



Otomobil Lastiklerinde Hava Basıncına Dikkat!

Sağlıklı ve güvenli sürüş için otomobilinizde lastiklere büyük görev düşüyor. bu yazımızda hava basıncı konusunda bilmeniz gerekenleri anlattık.

Lastik hava basıncı hakkında öncelikle belirtmeliyiz ki, her aracın her farklı modeline ve lastik ebadına göre değişiklik göstermektedir. Lastik hava basıncı yeni, sıfır otomobillerin kullanma kitapçıkların da her lastik ebadına göre hava Psi verileri kullanıcıya bildirilmiştir. Peki kullanma kitapçıkları olmayanlar hava basınç değerlerini nasıl öğrenir? Araç ön şoför kapısının iç kesiminde, yakıt depo kapağının iç kesiminde, bagaj içi gibi yerler de, lastik hava basınçlarının lastik ebatlarına göre kaç Psi olması gerektiği yazılıdır. Lastik hava basıncı değerleri Psi cinsinden yazılmamış olabilir. Özellikle Avrupa'da Psi değil, bar basınç değeri kullanılır. Peki Psi bar farkı nedir?

Psi Bar farkı

Psi ve Bar hava basınç değeri olarak görev gören iki ayrı birimdir. Bu değerlerden Bar değerinin kısaltılmışı olan b harfi ile simgelenir. Bar değeri dünya üzerinde kabul görmüş, Avrupa tarafından kullanılan basınç birimidir. Fakat dünyanın bazı bölgelerinde Bar yerine Psi birimi kullanılır. Peki, aracımız da basınç değeri Bar olarak verilmiş, lastik şişirme noktalarında ki makineler Psi birimi ise ne yapmalıyız? Bu sorunun cevabı çok basit. 1 Bar = 14.5 Psi değere eşittir. Bir örnek vermek gerekirse, aracımızda ki veriler bize 225 45 R17 lastik ölçülerine 2.6 Bar basınç uygulamamız gerektiğini söylüyor. Buradan yola çıkarak, 2.6*14.5 işlemi ile 37.70 sonucuna ulaşırız. 37.70 Psi basınç değeri 38 Psi değere yuvarlanır ve bu da demek oluyor ki, aracımızın lastiğine 38 Psi hava basıncı uygulayacağız.

Türkiye'de Psi değeri kabul görmüştür. Türkiye üzerinde gezip, görebileceğiniz tüm petroller de ki hava makineleri Psi değerleri üzerinden çalışır. Birçok işimizin yarım olduğu gibi, lastik hava basınçlarının kontrolünü yaptığımız petrollerde ki makineler de yarım yamalak çalışır durumda. Sizi yanıltabilir. En güzeli, Psi değerlerini düzenli şekilde bildiren lastik hava basıncı ölçen cihazlarla bir lastikçiye yaptırmak.

Dört lastiğin hava basıncı da aynı mı olmalıdır?

Yılan hikayesine dönmüş bir tartışmadır. Fakat otomobilinizin üzerinde ki verileri kontrol ederek bile, dört lastiğin basıncının da aynı olamayacağı kanaatine varabilirsiniz. Ön ve arka lastiklerin basınç değerleri yük durumuna göre birbirinden farklı olmalıdır. Yük durumu dışında elbette ki farklı faktörler de vardır. Bunlardan biri aracın yük dağılımıdır. Önden çekişli otomobillerin genel olarak yük dağılımı öndedir ve bu da ön lastiklerin basıncının arkalara nazaran daha yüksek olması gerektiğine işarettir. Özellikle BMW, Mercedes gibi arkadan itişli araçlarda hayat bulan, yüzde elli yüzde elli yük dağılımları aracın içerisinde ki yolcu sayısına önem vermemize sebebiyet verir. Arkadan itişli araçlarda genel olarak arka ve ön lastik hava basıncı Psi değerleri birbirine yakındır. Önden çekişli araçlar da yük dağılımı, motor, ön takım, alt takım ve birçoğu ön tarafta olduğu için ön iki lastik hava basıncı arka lastiklere nazaran daha fazla olmalıdır.

SIDE FACING OUTWARDS

Doğru lastik şişirme basıncı nedir ve bu bilgiyi nereden bulabilirim?

Aracınıza yönelik belirlenmiş lastik basıncı araç üreticisi ile lastik imalatçısı arasında belirlenmiştir. Araç/lastik kombinasyonunuza yönelik önerilen lastik basıncı bilgilerini araç el kitabında, yakıt deposu kapağında veya sürücü kapısı iç kısmında bulabilirsiniz.

Lastik basıncı araç performansının birçok önemli özelliğini etkiler, bu özellikler: Sürüş konforu, yönlenme dengesi, viraj alma, frenleme ve genel yol tutuş karakteristiği.

Doğru olmayan lastik basıncıyla sürüş, bu sayılan önemli özelliklerden bir veya birkaçını olumsuz yönde etkileyecektir.

Lastik şişirme basıncı nasıl kontrol edilmelidir?

Aracınızın lastiklerini araç ve lastik üreticisi tarafından belirlenmiş basınç değerine kadar şişirmelisiniz. Bu değer yük ve servis koşullarına bağlı olarak değişir.

Belirtilen basınç değeri daima SOĞUK lastik değeridir ve bu değerin altına düşmesine izin verilmemelidir. Sürüşün ısıyı yükseltmesinden dolayı sıcak lastiklerin içindeki basınç daha yüksek olacaktır. Bu yüzden asla sıcak lastiklerin içindeki basıncı düşürmeyin; çünkü bu lastikler soğuduğunda basınçları da minimum lastik basıncının altına düşebilir.

YAKIT TÜKETİMİNİ ETKİLİYOR

Lastik hava basıncının düşük olmasının bir diğer etkisi de yakıt tüketimine olacaktır.

Lastik basıncı (varsa yedek lastikler dahil olmak üzere) her 14 günde bir kontrol edilip ayarlanmalıdır. İlave yükler yüzünden lastik basınçlarının şartnameye göre artırılması gerekebileceğinden özellikle uzun bir tatile veya seyahate çıkmadan önce lastik basınçlarını kontrol edip ayarlamanız önem taşır.

Lastik Basıncı İzleme Sistemleri (TPMS)

1 Kasım 2014'ten itibaren Avrupa'da yeni araçların (kategori M1) tümüne Lastik Basıncı İzleme Sistemi (TPMS) kurulmalıdır. Lastik Basıncı İzleme Sistemleri farklı konseptler ve sensörlerden oluşabilir. TPMS sisteminin esas olarak 2 ana tipi mevcuttur:

Doğrudan sistemler - basınç sensörleri supaba entegre edilmiş veya janta ya da lastiğin iç kısmına monte edilmiştir.

Dolaylı sistemler - lastiğe/janta monte edilmiş herhangi bir basınç sensörü yoktur. Basınç farklılıkları, lastik dönüş çevresindeki değişimler gibi "dolaylı" yollardan ölçülür. Araba üreticileri, doğrudan veya dolaylı sistemleri kullanmayı tercih edebilirler.

TPMS sistemlerinin monte edilmesi ve bakımı lastik uzmanlarına bırakılmalıdır.

Lastiklerde Nitrojen Kullanımı

Nitrojen bazen lastik şişirmede havaya bir alternatif olarak sunulmaktadır.

Nitrojen bir inert (yanıcı olmayan) gazdır ve temel olarak oksijensiz kuru havadan başka bir şey değildir.

Havada %78 oranında nitrojen bulunur. Nitrojenin inert özelliklerinden dolayı, bu gaz önemli lastik servis uygulamalarında ve/veya uçak ve madencilik uygulamaları gibi zorlu koşullarda sıkça kullanılır. Nitrojen, motor yarışlarında da sıkça kullanılır.

Normal lastik servis uygulamaları için nitrojenle lastik şişirmenin gereği yoktur. Ancak, nitrojenle şişirme, lastiklere zarar vermez ve sızıntı yüzünden lastik basıncında azalmaları ciddi oranda düşürebilir. Buna rağmen nitrojen, lastik patlaması, lastik/jant arayüz (tel) sızıntıları, supap/jant arayüz sızıntıları, tekerlek sızıntıları vb. gibi nedenlerden dolayı hava kaybını önlemeyecektir.

İster normal hava ister nitrojenle şişirilmiş olsun, "önemli olan lastik basıncının düzenli takibidir."Yalnızca nitrojen basılmış olması düzenli lastik şişirme basıncı kontrolü yapılmasını engellemez.

Düşük lastik hava basıncı yakıt tüketimine etkisi

Lastik hava basıncı düşerse en belirgin sorun yakıt tüketimi olacaktır. Aracınızın lastik hava basıncını her hafta kontrol etmeniz önerilir. Yeni araçların birçoğun da lastik basıncının düşmesi arıza olarak bildiriliyor. Hatta hangi lastiğin basıncının düştüğünü ve kontrol edilmesi gerektiğini bile bildiriyor. Fakat eski model araçlar da bu sistem mevcut olmayabilir. Her hafta lastiklerin kontrol edilmesi gerekir. Özellikle uzun yola çıkmadan önce lastik basınçları kontrol edilmelidir. Uzun yola çıkmadan önce önerilen lastik Psi

Aşırı şişirmenin etkisi

AŞIRI ŞİŞİRİLMİŞ LASTİKLERLE SÜRÜŞÜN AŞAĞIDAKİLERE ETKİSİ OLUMSUZDUR:
Sürüş konforu, Yön dengesi , Özellikle hızlı girilen virajlarda, araç yol tutuş karakteristiği, Düzensiz aşınma

Yetersiz şişirmenin etkisi

YETERSİZ ŞİŞİRİLMİŞ LASTİKLERLE SÜRÜŞÜN AŞAĞIDAKİLERE ETKİSİ OLUMSUZDUR:
direksiyon tepkisi, yön dengesi
güvenli sürüş (viraj dönerken lastikler janttan çıkabilir)
ekonomi (daha fazla yakıt tüketimi daha az mesafe kat etme)
lastik dayanıklılığı.
düzensiz aşınma
EMNİYET UYARISI - Yetersiz şişirme, lastik yanak iç kısmının hasar görmesine neden olabilir. Bu durum lastiğin bozulmasına hatta parçalanmasına neden olabilir. Gizli lastik hasarları lastik basıncını ayarlayarak düzeltilmez.

değerleri 2 Psi kadar arttırılmalıdır. Yolun sonun da basınç değerleri yeniden kontrol edilmelidir. Lastikler soğukken bu kontrolün yapılması daha doğru olacaktır. Çünkü sıcak lastikler de Psi değerleri doğru sonucu vermeyebilir. Düşük lastik basıncı yakıt tüketiminin düşmanıdır. Yakıt tüketimi artışların da mutlaka ilk kontrol edilmesi gereken yer lastiklerdir.

Lastikleri petrollerin hava makinelerinden daha çok lastikçilerde yaptırmaya özen gösterelim. Birçok petrolün hava makinesi çalışıyor fakat yanlış çalışıyor. Sizi yanıltabiliyor ve yanlış yönlendirebiliyor.

Yakıt tüketimi sizin için de önemli bir faktör ise lastik hava basınçlarını mutlaka hafta da en az bir defa kontrol etmemiz veya ettirmemiz gerekiyor. Aksi takdirde Km.'de 30 kuruş yakıt sarfiyatında bulunan bir araç 50 kuruşa varan artışlar gösterebilir. Lastik hava basıncı zor kuralını ihlal etmemiş olmanıza rağmen savurabilir. Yola tutunamaz. Özellikle lastiklerinizin hava basıncı probleminin yanında bir de, eskimiş veya bitik olması çok kötü sonuçlar doğurur. Üzerinizde, virajı alırken kamyonla dönüyormuş hissi oluşturabilir.

Düşük lastik hava basıncı sonucu lastik patlaması

Lastiğin fazla şişirilmesi gibi lastik basıncının düşmesi de lastiğin patlama riskini yükseltir. Lastik hava basıncı düşük olan lastik yol üzerinde karşılaşabileceği katı cisimlere daha dirençsiz olacaktır. Lastiğin patlaması sonucu aracınızın kontrolünü kaybedebilir, yüksek hızlarda seyrediyorsanız kaza yapma riskiniz çok yüksek olacaktır. Yola çıkmadan önce kontrol edilmesi gereken ilk şey lastikler, ardından balatalar ve devamında su ve yağ benzeri motor bileşenleri olmalıdır.

Lastiklerinizin hava basıncını haftalık periyotta kontrol etmelisiniz.

ve pahalı bir konu değil, yalnızca özen gösterilmesi gereken bir durum. Ayrıca lastik ömrü için mutlaka havanın gereken düzeyler de olması gerekiyor. Aksi takdirde lastiklerinizin eskime süresi günden güne artacaktır.

Düşük lastik hava basıncı sonucu dengesizleşme

Hava basıncının herhangi bir lastikte düşmesi sonucu aracın tüm lastikleri eşit Psi değerlerine sahip olmayacaktır. Aynı olmayan lastik basınçları araç da denge problemine yol açacaktır. Farz edelim ki dört lastikte önlerden birinin basınç değeri 32 diğerinin 36 Psi. Arkalar dan biri 32 diğeri 34 Psi. Aracın lastiklerinin basınç değerleri birbirinden farklı olduğu için araçta dengesiz bir seyir hali söz konusu olacaktır. Yolda seyrederken sekmeler, sağa sola çekmeler, deniz üzerinde bir dalganın altınızdan geçiyor olması gibi hisler oluşacaktır. Bu da sizi kötü bir yolculuğun beklediği konusunda brifingler verir.

Düşük lastik hava basıncı yol tutuşu sorunu

Lastik basınçlarının birbirinden farklı değerlere sahip olması sonucu araç üzerinde özellikle uzun yolda yol tutuşu problemleri meydana gelebilir. Normalde 120 Km hızla dönebileceğiniz bir viraj, apex

Kış lastikleri için bu değerler nedir?

Soğuk havada dışarıdayken ortam sıcaklığına göre lastik hava basıncınızı doğru şekilde ayarlayabilmeniz için tavsiyeler:

Hava sıcaklıkları düştüğünde, lastik hava basıncınız da düşmektedir. Örneğin; bir lastik 20°C'de 2 bar (29 psi) şişirildiyse, lastik hava basıncı 0°C'de sadece 1,8 bar (26 psi) okunabilmektedir.

Soğuk havalarda dışarıdayken, ortamın sıcaklığına göre, lastiklerinizin hava basıncını ayarlamak istediğinizde, araç üreticinizin tavsiye ettiği hava basıncı değerlerine sadık kalmanızı öneriyoruz.

DÜŞÜK BASINÇ SORUNU

Lastik hava basıncının düşük olması kullanım konforunun yanı sıra sürüş güvenliğini de tehlikeye atabilir. Bu konuda dikkatli olun.

Araç üreticinizin belirttiği hava basıncı değerlerine;

- Aracınızın kullanım kitapçığında,
- Sürücü koltuğunuzun yanındaki yan kapının üzerindeki etiketlerde,
- Yakıt deposu kapağının iç yüzü üzerinde bulunan etikette bulabilirsiniz.

Soğuk havada içerideyken ortam sıcaklığına göre lastik hava basıncınızı doğru şekilde ayarlayabilmeniz için tavsiyeler:

Hava sıcaklığının lastiklerin hava basıncı üzerinde doğrudan etkisi bulunmaktadır. Lastik hava basınçlarınızı içeride, bir garaj veya atölye ortamında ayarlayacaksanız, araç üreticisinin tavsiye ettiği basınç değerlerine 0,2 bar (3 psi) ilave etmenizi öneriyoruz. Bu, içerideki atmosfer ile dışarıdaki sıcaklığı da dengeleyerek en doğru değeri bulmanızı ve aracınızı güvenle kullanmanızı sağlayacaktır.

Lastik rotasyonu

Lastik hava basıncı kontrolünüzde olduğu gibi, lastik rotasyonunu da ayda bir ve değişimi de aynı aks üzerinde yapmanızı öneriyoruz. Kış lastikleriniz için bu rotasyonun her 10.000 km ile 15.000 km arasında en az bir kere yapılmasını öneriyoruz. Lastik rotasyonu yapmanız lastiklerinizin dengeli şekilde aşınmasını sağlayacak ve kullanım ömrünü arttıracaktır.

Yolculuğunuz için tavsiyemiz: Lastik bakımı

Lastik hava basıncı ve bakımı, sürüş güvenliğinizi etkileyen başlıca faktörler arasında olmakla birlikte, bunların dışındaki ana etkenleri de hatırlamak gerekir. Örneğin; aracınızın ön camında bulunan bir çatlak soğuk havalarda çok büyük bir kırığa dönüşebilir ve güvenliğinize karşı bir tehdit oluşturabilir. Bu nedenle mutlaka aracınızın ve lastiğinizin gerekli kontrollerini yaptırmanızı öneririz.

Ayrılıklar Online Hayatı Tehdit Ediyor

İnternet hesapları ve bağlantılı cihazların günlük yaşantımızdaki rolü arttıkça, bir ilişki içerisindeki insanların özel hayatlarının sınırlarını belirlemesi giderek zorlaşıyor. Peki çiftler ayrıldığında ne oluyor?

Dünya genelinde yapılan araştırmaya Türkiye'den katılanların yüzde 28'i, eski eşlerine internet hesaplarından erişebildiklerini belirtti. Yani ayrılıklar online hayat için büyük bir risk haline dönüşüyor. Terk edilen kişilerin intikam almak isteyebileceği düşünüldüğünde, bu günümüzde ayrılıkların ardından eşlerin karşı karşıya kaldığı risklerin yalnızca görünen kısmı.

Dijital sınırlarla belirlenen dünyada, özel hayat giderek daha da esnek bir kavram haline geliyor ve online hayat önemli bir risk faktörü olarak konumlanıyor. İlişkiler de buna dahil. Örneğin, Türkiye'de çiftlerin Yüzde 82'si kişisel cihazlarına erişim için kullandıkları parolalarını, PIN'lerini veya parmak izlerini paylaşıyor.

Eşlerin cihazlarında hassas bilgiler bulunuyor

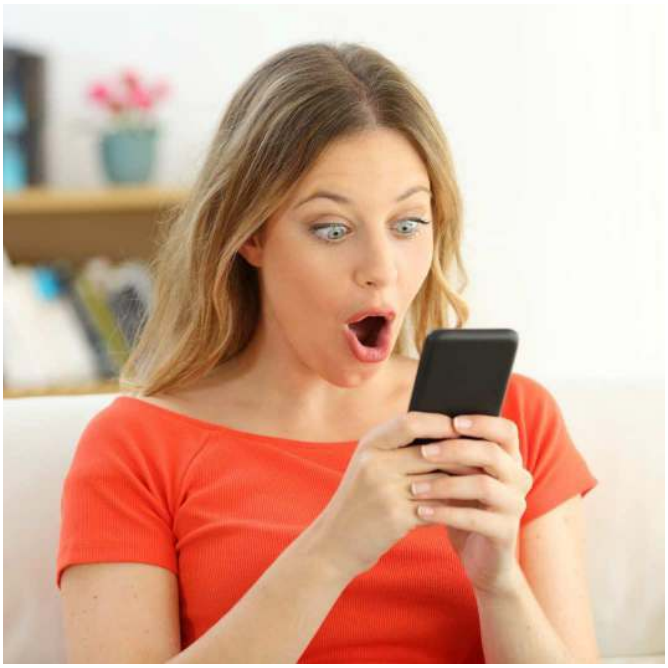
Yüzde 21'lik bir kesim ise eşinin cihazında özel ve hassas verilerini saklıyor. Bunlar arasında eşler arasındaki özel mesajlar (yüzde 8), kendilerinin samimi ve özel fotoğrafları (yüzde 9), kendilerinin ve eşlerinin samimi videoları (yüzde 10) yer alıyor. Buna ek olarak kullanıcılar eşleriyle paylaştıkları hesaplarda ve cihazlarda, finansal bilgiler (yüzde 10) veya işle ilgili bilgiler (yüzde 10) gibi kritik veriler de saklıyor.

İlişki düzgün bir şekilde yürüdüğünde ve veriler güvenilir ellerde olduğunda bunların hiçbir sakıncası yok fakat ayrılık söz konusu olduğunda online hayat için bazı önemli sorunlar ortaya çıkıyor. İlişki kötüye gitmeye başladığında, cihazlarda veya internet hesaplarında samimi anıların paylaşılmış olması, yakın bir ilişkinin doğal bir parçası olmaktan çıkıp potansiyel bir kabusa dönüşebiliyor.

İntikamcı eski eşler büyük tehdit

Türkiye'de ayrılık yaşayanların yüzde 11'i intikam olarak eski eşlerinin özel bilgilerini paylaştığını veya paylaşmak istediğini, yüzde 11'i eşinin cihazına hasar verdiğini veya vermek istediğini ve yüzde 28'i ise erişebildikleri hesapları gizlice izlediğini belirtti. Türkiye'deki katılımcıların yüzde 8'inin internette eski eşinin parasını harcadığı göz önünde bulundurulduğunda, tüm bunların potansiyel bir maddi etkisinin de olduğu görülüyor.

İlginç bir şekilde, ayrılık



sonrası verilen tepkilerde cinsiyetler arasında bazı gözle görülür farklar bulunuyor. Erkekler intikam olarak eski eşlerinin kişisel bilgilerini açığa çıkarmaya (yüzde 13'e karşı yüzde 8) ve bu bilgilerden faydalanmaya (yüzde 15'e karşı yüzde 9) kadınlara göre daha yatkın görünüyor. Kadınlar ise ayrılık sonrasında eşlerine ait tüm bilgileri kendi cihazlarından kaldırmayı (yüzde 76'ya karşı yüzde 60) ve ortak fotoğrafları veya videoları silmeyi (yüzde 79'a karşı yüzde 65) erkeklere kıyasla daha çok tercih ediyor.

Kadınlar eski eşlerini izliyor

Ancak kadınlar bazı gizli taktikler uygulamaktan da kaçınmıyor. Kadınların yüzde 45'i eski eşlerinin sosyal medya hesaplarını gizlice izlediğini kabul ederken, erkeklerde bu oran yüzde 37'de kalıyor.

Dijital dünya, çiftlerin iletişim kurması için harika imkanlar sunmasının yanı sıra ayrılık durumunda da özel hayatı önemli risklerle karşı karşıya bırakıyor. Bireylerin önemli bir kısmı eski eşlerine ait hassas verileri kötüye kullanmaya yatkın görünüyor.

Bu nedenle kullanıcılar hassas veriler paylaştığında her zaman çok dikkatli olmalı ve bu verilerin nerede saklandığını tam olarak bilmeli. Ayrıca konu özel hayatın gizliliğiyle ilgili bir soruna dönüşmeden önce, verilerin kime ait olacağını belirlemek için bir dijital sözleşme de yapılabilir.

Ayrılıkların ardından özel hayatınızın gizliliği risk altında kalmak zorunda değil. Kullanıcıların, eski eşlerinin erişebildiği hesaplara ait parolaları mutlaka değiştirmesi gerekiyor.

Öyleyse Bırakın!

İlişkilerde sosyal medya olumsuz pek çok etki ortaya çıkarıyor. Sosyal medyada zaman geçirmenin size iyi gelmediğini düşünüyorsanız bunu sınırlamak, sınırlayamıyorsanız en azından bir süreliğine hesaplarınızı dondurmak veya kapatmak faydalı bir çözüm olabilir. İnternet kullanımınızı genel olarak kısıtlamak istiyorsanız, bu konuda teknolojiden yardım alabilirsiniz. Bilgisayar ve telefon uygulamaları bulunan Freedom (freedom.to) bu çözümlerden biri. Uygulama internet erişiminizi önceden belirlediğiniz bir süre için kısıtlıyor. Tabi işiniz veya sosyal hayatınız her an online olmayı gerektiriyorsa bu tarz çözümler biraz zorlayıcı olabilir. Bunun yerine, önceden belirlediğiniz siteleri belirlediğiniz zaman dilimlerinde erişime engelleyen Anti-Social (anti-social.cc) adlı yazılım/uygulamayı da deneyebilirsiniz.

Güvenlikte Yükselen Trend: Biyometri Teknolojisi

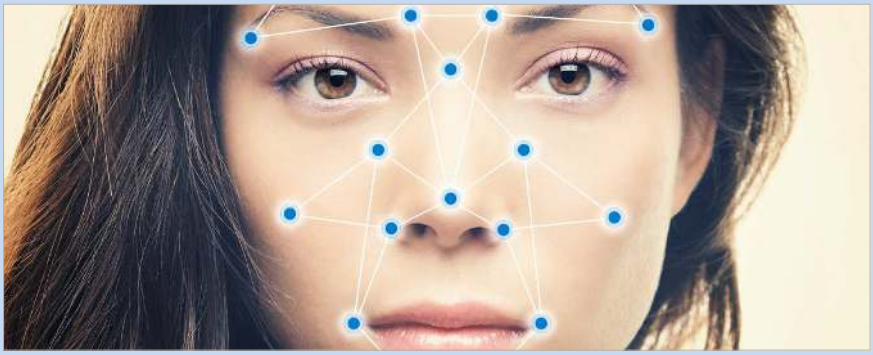
Şifre kullanmaktansa biyometrik bilgileri kullanmak, yeni dönemde en güvenli, pratik, ekonomik ve hijyenik yöntem halini aldı. Bu yazımızda, biyometri teknolojisine hızlı bir bakış atıyoruz.

Yüz tanıma Hızlı ve Güvenli Çözüm

1960'ların ortalarında Woody Bledsoe, Helen Wolf ve Charles Bisson yüz tanıma tekniklerini araştırmaya başladılar. Optik taramalardan alınan karakteristik özellikleri dijital veya vesikalık fotoğraflarla eşleştirmeyi denediler. Ancak o dönemin teknolojileriyle eşleştirme işleminin sağlıklı şekilde yapılamadığı ortaya çıktı.

Günlük yaşamımızda kullanılabilen uygulamalar onlarca yıl sonra, 1997'de ortaya çıkmaya başladı. Bochum teknolojisini (Christoph von der Malsburg ve öğrencileri tarafından Almanya'daki Bochum Üniversitesi'nde geliştirilmişti.) kullanan sistemlerin denemelerde iyi sonuçlar verdiği ortaya çıkmıştı. Bu teknolojinin en kritik yönlerinden birisi, mükemmel çekilmemiş fotoğraflarda da işe yaraması ve gözlük, sakal, bıyık gibi özelliklerden etkilenmemesiydi. ZN-Face adıyla satılan ürün, Deutsche Bank ve havalimanları tarafından kullanıldı.

Amerikalı Identix firması, 2007'de duyurduğu FaceIt teknolojisiyle yüz tanımayı bir adım daha ileri götürdü. FaceIt, özel bir algoritma kullanarak iki boyutlu görsellerden üç boyutlu yeni görseller oluşturabiliyor. Bu yöntem sayesinde FaceIt, kişileri internetteki fotoğraflarından veya tren istasyonu, futbol sahası gibi kalabalık yerlerde bile fark edebiliyor. Bu gelişme sayesinde FaceIt ve benzeri yazılımlar CCTV (kapalı devre kamera sistemleri) video izleme sistemleriyle bütünleşmeye başladı. Tüketici ürünü tarafında, PlayStation 4 oyun konsolunda yüz tanıma özelliği bulunuyor.



Parmak izi

Basit ve Geleneksel

Parmak izini imza olarak kullanmak binlerce yıl geriye, Babil zamanlarına kadar gidiyor. Bu uzun tarihçenin bir yerinde, birisi; her insanın parmak izinin eşsiz kavislere, sarmallara ve döngü motiflerine sahip olduğunu fark etmiş. FBI'ın Kimlik Tanımlama Bölümü 1924 yılında kuruldu ve o zamandan beri de parmak izlerinin veritabanı tutulmaya başlandı. 1946'da 100 milyona yakın parmak izini toplamayı başarmışlardı. 1980 yılında ise Automated Fingerprint Identification System (AFIS: Otomatik Parmak İzi Tanımlama Sistemi) projesi yardımıyla tüm kataloğu dijital hale getirdiler. Günümüzde ise bu işe özel parmak izi algılayıcıları bilgisayar klavyelerinde, farelerde ve yeni nesil akıllı telefonlarda bulunabiliyor.

Abores antur abor aut expliquae. Itatem nobit et ut et modis et etur? Namus cupta volorem eatiur, quis num etus magnatibus sequisti re

DNA profilleme

En Gelişmiş Yöntem

İsviçreli doktor Friedrich Miescher, ameliyat sargılarındaki kalıntıları inceleyip deoksriboükleik asidi (DNA) ayrıştırarak bir ilke imza attı. Phoebus Levene, DNA'nın nükleotid elemanlarının belirli bir yapıya sahip olduklarını öne sürmüş, James Watson ve Francis Crick 1953'te çifte sarmal modelini anlattıkları makaleyi yayımlayıp Nobel Ödülü'nü alana kadar bulmaca çözülememişti. DNA profilleme (veya genetik parmak izi alma), büyük olasılıkla en gelişmiş biyometrik kimlik tanımlama yöntemi. DNA örneklerinin analizine dayanan olay yeri inceleme çalışmaları, 1984 yılında İngiliz genetikçi Sir Alec Jeffreys tarafından geliştirildi.

Abores antur abor aut expliquae. Itatem nobit et ut et modis et etur? Namus cupta volorem eatiur, quis num etus magnatibus sequisti re

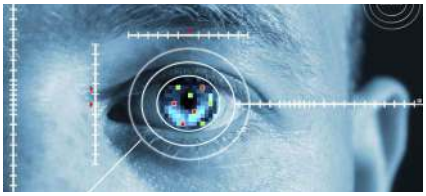
İris tanıma Yakın Geleceğin Kimlik Tanıma Teknolojisi

1949 yılında İngiliz göz doktoru James Hamilton Doggart, incelediği her irisin diğerlerinden farklı bir yapıya sahip olduğunu fark etti. Doggart, bu mimarideki dizilim ve olasılıkların neredeyse sonsuz olduğunu öne sürdü.

1980'lerde Amerikalı göz doktorları Leonard Flom ve Aran Safir, iris tanımlama kavramının patentini aldı. Ancak, çalışan bir iris tanıma çözümünü ilk geliştiren kişi, 1994 yılında, Cambridge Üniversitesi Bilgisayar Laboratuvarı'nda bilgisayarla görme ve doku tanıma üzerinde çalışan Prof. Jhon Daugman oldu.

Daugman'ın patentini aldığı ve resim işleme, özellik çıkarımı, doku eşleştirme amacıyla kullanılan bilgisayarla görme algoritmaların lisansı birçok şirkete satıldı. Bu şirketlerden biri de Flom, Safir ve Dougman tarafından kurulan IriScan idi.

Günümüzde iris tarama teknolojisi çoğu ülkenin göçmenlik büroları ve sınır kapılarında kullanılıyor. UIDAI (uidai.gov.in) projesi, Hindistan'daki 1,2 milyarlık nüfusun hepsinin iris kayıtlarını toplamak adına Hindistan'da sürdürülüyor ve bu alandaki en büyük proje.



Siber Güvenlik Alanında Çalışmak İsteyenler İçin Başlangıç Rehberi

Bireyler, şirketler ve devletler için öncelikli konulardan biri olan siber güvenlik, kimileri için kariyer fırsatı olabilir. Bu dosyamızda temel bilgileri paylaştık.

Siber güvenliği, sıradan insanların uzak durması gereken, kendine has, ender bir kariyer olarak görüyor olabilirsiniz. Fakat durum farklı. Dijital çağın günlük hayatımıza hızla sindiği bu zamanlarda, kariyeriniz ne olursa olsun, herkes mutlaka bir nebze de olsa temel bir siber güvenlik anlayışına sahip olmalıdır. Bu sayede şirketler iş yerinde dirençli bir görev protokolü yürütebilirler. Evde ise kendi bilgilerinizi korumak daha kolay olacaktır.

Teknoloji modern hayatı her açıdan etkiliyor

Güvenlik öğreniminin neden bu kadar önemli olduğunu anlatmaya başlarken, isterseniz önce günlük hayatın pek çoğumuz için nasıl geçtiğine bakalım. "Modern teknolojiden faydalanmayan meslek nerdeyse kalmadı." Bu sözlerin sahibi olan Virtustream güvenlik şefi Matt McCormack'e biraz kulak kabartalım:

"Öğretmenler SMART sınıf tahtalarını kullanıyor. Tamirat veya bakım için evinize gelen bir kişi bir akıllı telefonu veya tableti çıkarır ve oradaki bir uygulamaya bilgi ekler. Şirketlerde en fazla hasara neden olan hatalar güvenlikle ilgilidir. Bu problemlerin nedeni, güvenli olduklarını bilmeden e-postalardaki eklere tıklamak kadar küçük bir şey olabilir."

Ayrıca, güvenlik endişeleri sadece iş yeriyle de sınırlı kalmıyor: "Günümüzde artık sadece şirketinizin güvenliği değil, kendi güvenliğiniz ve sosyal ağlarda neler paylaştığınız da önemli bir konu. Hükümet için çalıştığım zamanlarda, iş hayatı dışında olsa bile, her zaman insanlara sosyal medyada ne yapmamaları gerektiği yönünde tavsiyelerde bulunurduk."

Temel güvenlik bilgisi her kariyerde işe yarar

Basit bir şekilde şüpheli e-posta eklentilerine tıklamamak iyi bir başlangıç olacaktır. Fakat neredeyse tüm çalışanlar, şirket güvenliğini artıracak ve kendilerine değer katacak bir takım şeyler yapabilir. LinkedIn bilgi güvenliği yöneticisi Pavi Ramamurthy: "Kurum içindeki herhangi bir rolde, güvenlik hakkında bilgi edinmek, bireyin riskleri anlamasına ve kritik durumlarda bilinçli kararlar vermesine yardımcı olur."

Siber saldırılar insan hatasına dayanıyor

Siber saldırganlar güvenlik ihlalleri için sadece yeteneklerine güvenemezler. Gerekli olan diğer şeylerin başında insan hatası gelir. Ph.D. profesör ve RIT bilgisayar güvenliği şefi Bo Yuan şunları söylüyor: "2017'nin ilk çeyreğinde şirketlerin karşılaştığı tehditlerle ilgili bir analize göre, siber saldırganlar büyük oranda kullanıcı etkileşimine gereksinim duyuyor.

Çarpıcı bir örnek vermek gerekirse: Equifax CEO'su, 2017'deki saldırıda ihmali bulundu. Evet, 147 milyon müşteriyi etkileyen ve 600 milyon dolarlık zarar oluşturan saldırının nedeni insan hatasıydı. "Bilişim sektöründe çalışmayan fakat iş için bilgisayarlı aygıt kullananların temel güvenlik eğitimi almaları, ufak bir hatanın veya göz kaçırmanın nasıl felaketlere yol açabileceğini anlamları için önemlidir. Eğitim, saldırıların giderek karmaşıklaşıp ve gelişkin bir hal alması yüzüden, güvenlik zafiyetlerini azaltmada insan hatasını minimuma indirmede hayati önem taşır."

Güvenlik bilgisiyle çalıştığınız iş yerinde ilerleyebilirsiniz

İşinizde ilerlemek için yeni beceriler kazanmak güvenli bir yoldur. Güvenlik dalı da şu sıralar son derece uygun. Kendini siber güvenlik alanında eğitmek, ortalama bir çalışanın kariyerinde olumlu bir etki yaratacak. Hiyerarşide yükselmek veya zam almanın ilk adımı, ek sorumluluklar almada güvenilir olduğunu göstermektir. Işiniz doğrudan bir güvenlikçi rolü üstlenmese de, çalışma ortamınızın kötü niyetli bir üçüncü şahıs tarafından

istismar edilme yollarını düşünün.
Mesela, şüpheli link içeren e-postanın sahibine teyit etmek için e-posta gönderin. Uzun linkleri kısaltıp daha okunur hale getirmek için Google'ın https://goo.gl URL hizmetinden haydalanabilirsiniz. Fakat bu yolla kötü bir aktör, kötü niyetli bir siteye bağlanan yanıltıcı bir goo.gl URL'si kullanarak çalışanları hataya düşürmeye çalışabilir. Sıradan kullanıcıların bu tür tuzaklara düşme ihtimali çok daha yüksek

Çalıştığınız şirket güvenlik eğitimi için gerekli harcamaları karşılamak istemese bile kendi kendinizi eğitebilirsiniz. Diplomalı, sertifikalı, plaketli resmi bir eğitim almanız da gerekmiyor. İşin aslı, dünya hakkındaki düşünme biçiminizi genişletmek ve bu sayede kendinizi kötü adamların yerine koyarak olası zafiyetleri erkenden keşfetmektir.

Şimdi güvenlik eğitimi alarak ileride harika bir kariyere ulaşabilirsiniz
Güvenlik ile ilgili araştırmalarınızdan zevk aldığınızı ya da ilgili becerilerin ilginizi çektiğini keşfederseniz, neden bu tam zamanlı bir kariyer olmasın? Şimdi böyle bir adım atmak çvresel koşullar son derece müsait. Bir araştırmaya göre, 2021 itibariyle 3,5 milyonluk bir siber güvenlikçi açığı oluşması bekleniyor. Bu tür bir rağbet, kariyer sıçraması yaşamak isteyen herkesin üzerinde düşünmesi gereken bir konu.

Bu sayede başarıyla sonuçlanan hikayelerin sayısı hiç de az değil. Bu kişilerden birisi de, kendi güvenlik kariyeri için meslek değiştiren ve şu an Ping Identity'de yönetici teknik mimar olan Sarah Squire. Kariyerine web geliştirici olarak başlayan Sarah bir süre sonra ufak bir bilgi güvenliği takımı tarafından işe alınır. Bir yıllık yorucu bir eğitimin ardından bu mesleğe adeta aşık olur. Sarah, bu küçük platformu kullanarak yeni bir vasıf kazanır ve sonra kendi danışmanlık şirketini kurar. Bu noktadan sonra

işini ilerletir ve artık NIST rehberlerine katkıda bulunmak, şöhretli güvenlik konferanslarında konuşmak, eğitim kitapları dokümanları hazırlamak ve herkesin internette günlük kullandığı iletişim protokolleri için fikir sağlamak gibi görevlerin altından kalkacak duruma gelir.

Görece kısa süreli bir eğitim ile Sarah Squire tüm kariyer eğrisini tepeye çevirmeyi sağladı. Sizin de böyle bir kariyer sıçraması yaşamamanız için hiçbir engel yok.

SİBER GÜVENLİKÇİ GÖREV LİSTESİ

- Satışlarda, kurumun güvenlik duruşu hakkında müşterilere güvence verin.
- Şirket iletişimlerinde, durumu sektörel saygınlık ve marka güveni ekseninde değerlendirmelisiniz.
- Hukuk danışmanlarınız, tedarikçi ve müşteri antlaşmaları çerçevesinde oluşturulan güvenlik şartlarının doğruluğundan emin olmalıdır.
- İnsan kaynaklar ve/veya güvenlik takımı için, daha iyi güvenlik farkındalığı ve eğitim için gerekli koşulları öğrenin.
- Ürün yöneticileri, iyi güvenlik seçenekleri tavsiye etmelidir.
- Mühendislik projelerinde güvenli kod geliştirdiğinizden emin olun.
- Güvenlik uzmanları, çalışabilirlik ve güvenlik teyidi için incelemeler ve kalite kontrol testleri yürütmelidir.
- Şirket yönetimi, bir güvenlik olayında doğrudan devreye sokabilecekleri ve zafiyeti en hızlı şekilde tespit edebilecekleri bir savunma planı bulundurmalıdır.

Gördüğünüz gibi, güvenlikle ilgili projelerine katkı sağlamak ve farkında olmak için herkesin bir güvenlik uzmanı olması gerekmiyor. Aslında, ne kadar çok personel belli bir güvenlik farkındalığı seviyesinin üstünde bulunursa, güvenlik ihlallerinde o kadar az para ve zaman kaybedersiniz.

"Kampanya" Tuzaklarına Düşmeyin!

Sosyal medya kanalları ve mobil uygulamalar üzerinden son günlerde artan sahte kampanyaların cazibesine kapılıp, dolandırıcılara şifrenizi ve finansal bilgilerinizi kaptırmayın, ucunun nereye varacağını bilmediğiniz 'link'leri tıklamayın ve paylaşmayın.

Sosyal medyada çok sayıda güvenilir markanın unvan, logo ve benzeri kurumsal kimlik bilgileri kullanılarak ve internet siteleri taklit edilerek sahte kampanya kurgularıyla yapılan dolandırıcılık girişimlerine karşı dikkat! Tüketicilerin bu tür girişimlerden korunmaları için kampanya içeriğini ilgili markanın orijinal ve güvenilir internet sitesinden kontrol ve teyit etmesi büyük önem taşıyor.

Siber suçlular organize ediyor

Dolandırıcılığın çalışma prensibi oldukça basit. Sosyal medya kullanıcılarına, bilindik pek çok markaya ait sahte indirim kuponları veya hediye çekleri kullanımı içeren mesajlarla birlikte 'link'ler iletiliyor. Kullanıcılar bu 'link'lerle markaların sitelerine birebir benzeyen sahte sitelere yönlendirilerek, kişisel ve finansal bilgileri elde edilmeye çalışılıyor.

Nasıl yapılıyor ve ne hedefleniyor?

Kullanıcıların karşılaşabileceği durumlar insanların korku, heyecan, heves gibi belli duygularını kontrol altına almak isteyen 'sosyal mühendislik' yöntemleri neticesinde şifre ve kullanıcı bilgilerinin ele geçirilmesini hedefliyor. Sosyal medya kanalları dışında dolandırıcıların kullandığı senaryolardan birkaç tanesi şöyle:

- Hesabınızdan/kartınızdan işlem gerçekleştirilmiş. İşlemi iptal etmek/iade almak için şifrenizi söyleyiniz/tuşlayınız.
- Hesaplarınıza Rusya'dan siber saldırı gerçekleştiriliyor. Hesaplarınıza bloke koymak için şifrenizi söyleyiniz/tuşlayınız.
- Geriye dönük kredi/kredi kartı ücretlerini iade edeceğiz. İşlemi gerçekleştirmek için şifrenizi söyleyiniz/tuşlayınız.
- Sigorta primlerinizi iptal edeceğiz. İşlemi gerçekleştirmek için şifrenizi söyleyiniz/tuşlayınız.

SAHTE KAMPANYALARDAN VE DOLANDIRICILARDAN NASIL KORUNABILIRSINIZ?

Kart ve bankacılık işlemlerinizi daha güvenli gerçekleştirip bilgilerinizi korumak birkaç küçük tedbir ile mümkün. Tüketicilere cazip teklifler sunan, inandırıcı senaryolarla kişisel ve finansal bilgilerine ulaşmayı hedefleyen bu tür dolandırıcılık girişimlerine karşı aşağıdaki önerileri dikkate almalarını tavsiye ediyoruz:

1. Şifrenizi ve finansal bilgilerinizi her ne olursa olsun telefon, SMS veya e-posta aracılığıyla size ulaşan kimseyle paylaşmayın/tuşlamayın.
2. Herhangi bir kampanya içeriğinin ilgili markaya ait olup olmadığını, markanın orijinal ve güvenilir internet adresinden kontrol edin.
3. Kampanya içeriğinde kullanılan bağlantının ilgili markanın orijinal ve güvenilir internet adresiyle birebir aynı olduğundan emin olun.
4. Banka logosu ve adı kullanılsa dahi kişisel bilgilerinizi isteyen e-postalara ve sitelere yanıt vermeyin.
5. SMS ile gelen şifrelerinizi, kart bilgilerinizi kimseyle paylaşmayın/tuşlamayın.

EVLERDE YANGINA KARŞI 10 TEDBİR

1

Tavan arası ve bodrum katlarını temiz tutmaya özen gösterin.

2

Çocukların ateşle oynamasına izin vermeyin, onları bu konuda uyarın.

3

Soba, kalorifer ve mutfak ocakların kullanımında kurallara uyun ve dikkatli olun.

4

Yanıcı maddeleri evinizin korunaklı, ateş almayacak bir yerinde saklayın.

5

Elektrik tesisatından çıkabilecek yangınlara karşı düzenli bakım yaptırın.

6

Sıvasız, çatlak, hatalı inşa edilmiş ve dolmuş bacaları kullanmayın

7

Evinizin mutfak, salon ve yatak odasında yangın söndürme tüpleri bulundurun.

8

Olası yangın durumunda nasıl tahliye olacağını planlayın ve tatbikat yapın.

9

Yangından ilk aşamada haberdar olmak için farklı odalara duman dedektörün koyun.

10

Yangınlarda kayıpların %75'i duman zehirlenmesinden. Kişi sayısı kadar gaz maskesi edinin.

Kurumsal Siber Güvenlikte %100 Yerli Çözüm:

berqNET

Şirketlerin en önemli gündem konularından biri dijitalleşme. Tüm iş süreçlerini daha verimli biçimde elden geçirmek ve tamamen dijitalleşmek beraberinde bazı tehditler de doğruyor. Şirketlerin kurumsal olarak siber tehlikelere karşı kendilerini ve müşterilerini korumaları için ek yatırımlarda bulunması şart. Logo Yazılım desteğiyle kurulan berqNET, Türkiye'deki her boyutta işletmeye %100 yerli siber güvenlik çözümleri sunuyor.

Tüm işletmelerin siber güvenlik ihtiyaçlarını çözmek için tasarlanan berqNET'i; Restoran ve kafelerden öğrenci yurtlarına, otellerden belediye kurumlarına, üretim tesislerinden enerji santrallerine, devlet kurumlarından özel işletmelere, küçük bir avukatlık bürosundan orta boyutlu bir müşavirlik firmasına kadar büyüyen, büyümek isteyen ve iş süreçleri içinde internet bulunan herkes kullanabilir.

BERQNET NE GİBİ HİZMETLER VERİYOR?

Tüm Türkiye'de 500'den fazla bayisiyle 5.000'den fazla işletme tarafından tercih edilen ve Türkiye'nin lider firewall'u olma vizyonuyla çalışmalarına devam eden berqNET'in sunduğu özellikleri şöyle sıralayabiliriz:

- Bütünleşik Güvenlik Hizmeti
- Basit, Anlaşılır ve Türkçe Kullanıcı Arayüzü
- Mobil Uygulama Aracılığıyla İstenilen Her Yerden Rapor Görüntüleme ve Cihaza Uzaktan Erişim İmkanı
- Hotspot Özelliği
- İleri Düzey Web ve Uygulama Filtreleme Özellikleri
- 5651 sayılı yasaya uygun kayıt tutma çözümü
- VPN Hizmetleri (IPSec, SSL)
- IPS (Saldırı Engelleme Sistemi)
- İleri seviye raporlama özellikleri
- Yerleşik Antivirüs Koruması
- WAN Balancing (İnternet Yük Dengeleme Sistemi)
- Farklı markalar ve ürünlerle hızlı entegrasyon olabilme kabiliyeti
- %100 Yerli AR-GE
- Müşteriye özel teknik destek hizmeti: İster telefonla ister online

RAKAMLARLA TÜRKİYE'DE KURUMSAL SİBER GÜVENLİK

- Türkiye, en çok siber saldırıya maruz kalan Avrupa'da 1, Dünyada 6. Ülke
- Ülkemizde yaklaşık 500 binden fazla zararlı içerik bulunduran web sitesi bulunuyor.
- Türkiye'deki kullanıcıların, her ay 3 ve 7 milyon arasında zararlı içeriğin bulunduğu siteye girmesi engelleniyor. Bu sayı, tüm dünyadaki web sitelerinin yüzde 1,7'sine denk geliyor.
- Türkiye'de belirlenen zararlı yazılım sayısının 1.5 milyon civarında olduğu açıklandı
- Türkiye'ye haftada 18 bin ciddi siber saldırı yaşanıyor
- 2017'de fidye saldırısının en çok yapıldığı ülke Türkiye. Hedefteki kullanıların büyük bölümü ise küçük ve orta boyutlu işletmeler yani kobiler
- İşletmelerin Siber Güvenlik çözümlerini efektif kullanmamalarından doğan verimlilik kaybı: %40 (Gartner Verilerine göre)
- Bir IT yöneticisinin siber güvenlik ürününden beklediği öncelikli özelliklerin başında kolay ve anlaşılır yönetim geliyor. (Kaynak: Gartner)

PARMAK İZİ GÜVENLİĞİ HAKKINDA DOĞRU BİLİNEN YANLIŞLAR

Günümüzde en yaygın güvenlik yöntemlerinden biri haline gelmeye başlayan parmak izi hakkında bilmeniz gerekenler bu dosyamızda.

Dijital güvenlik konusunda parmak izleri uzun zamandır nihai bir tamamlayıcı olarak görülüyor. Parmak izi okuyucular bir süredir artık akıllı telefonlara da entegre oldular. Parmakların tamamen kişiye özel ve çalınması imkansız olması nedeniyle parmak izi okuyucularının çok güvenli olmaları bekleniyor. Ama görünen o ki, tam olarak da öyle değiller.

EFSANE 1:
Parmak izleri, parolalardan daha güvenlidir.

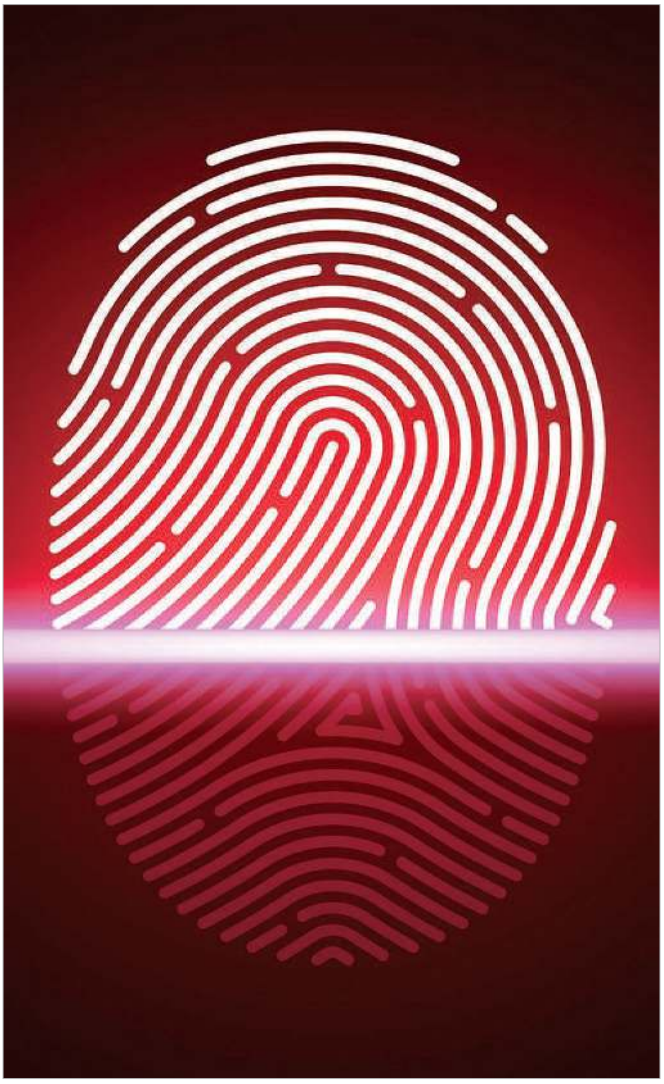
Birçok insanın düşündüğünün aksine biyometrik okuyucular hatasız değiller. Kendilerine has açıkları, zayıf noktaları var, kandırılabilirler. Ayrıca izleri çalınabilir hatta bir fotoğraftan bile kopyalanabilir.

EFSANE 2:
Parmak izi kopyalanamaz

Apple 2013 yılında iPhone 5s'e parmak izi okuyucu dahil ederek yeni bir çığır açtı. Hem telefonunuzun süper koruma altında olacağını hem de Touch ID kullanarak iTunes ve Apple Store üzerinden parola girmeye gerek kalmadan kolaylıkla alışveriş yapabileceğinizi vaat etti.

Fakat gelin görün ki daha iPhone 5s'in piyasaya çıkmasının üzerinde iki gün geçmişti ki, kendine Starburg diyen bir Alman güvenlik araştırmacısı, herkesin indirebileceği bir yazılım olan VeriFinger'ı kullanarak Alman İçişleri Bakanı'nın parmak izlerini kopyaladı. Hem de yüksek çözünürlüklü fotoğraflardan faydalanarak.

Daha günceli; 2016 yılında Biyometrik firması Vkansee, teknolojinin kandırılabileceğini gösterdi.



FBI'da 100 milyon kişinin parmak izi var

Amerika'yı ziyaret eden 14 – 79 yaş arasındaki herkesin parmak izinin alınması kanuni bir zorunluluktur. Bu arada FBI'ın elinde yaklaşık 100 milyona yakın insanın parmak izi dosyası bulunuyor, üstelik bunların 30 milyondan fazlası hiç suça bulaşmamış insanların izi. Söz konusu bu örnek, suçluların erişimine açık olabilecek özel bilgi depolarının varlığını gösteriyor. Eğer bilgiye erişilebiliyor ise, o bilgi çalınabilir ve aynen kredi kartlarında olduğu gibi suçlular tarafından kullanılabilir.

Tek yapmanız gereken biraz kil ve biraz oyun hamuru edinmek. Bu şekilde sensörleri kandırmaya yetecek kadar detaylı parmak izleri edinmek gayet de mümkün oluyordu.

EFSANE 3:
Parmak izleri gelecekte parolaların yerini alacak.

Parmak izlerinin kopyalanarak cihazları kandırmak için kullanılabileceklerini düşünürsek, parolaların yakın zamanda işlevsiz hale gelmesi pek de mümkün görünmüyor.

SONUÇ

Altı çizilmesi gereken nokta; tek bir çözüm hiçbir zaman tam güvenlik sağlamayak. Birçok uzman birden fazla güvenlik önlemi alınması gerektiğinde birleşiyor. Çünkü korumakta olduğunuz veriye birden fazla erişim yolu bulunuyor. Pratik hayatta parmak izi, parola ve iki faktörlü doğrulama gibi yöntemlerin kombinasyonu en doğru yol olacaktır. Özellikle de erişilmesini istemediğiniz fiziksel veya dijital veri çok önemli ise.

OKULLAR NANO TEKNOLOJİYLE TERTEMİZ

Hayatımızın her alanında giderek daha fazla yer alan nano teknoloji uygulamaları ve ürünleri, sağlığımızla ilgili konularda da etkin hale geliyor. ISS Haşere Kontrol ve Bitki Bakım, uzman bir ilaçlama şirketi olarak NanoClear ürünü ile ilaçlama yapıyor ve okullar başta olmak üzere bütün toplu yaşam alanlarına gerçek hijyen hizmeti sunuyor.

Bir eğitim dönemi daha bitiyor ve velilerin bir bölümü için yeni okulda yeni yaşam gündemde. Bütün veliler gibi okul yönetimlerini de çocukların eğitim göreceği alanlarda hijyen koşullarının sağlanmasından endişe ediyor. Çünkü tıpkı hastaneler gibi okullar da kalabalık kitleler bir arada bulunduğu için hastalık üreten her türlü mikrop, zararlı bakteri ve parazitin yayılmasına elverişli ortamlardır.

Yapılan araştırmalar, okulların, okul kantinlerinin, okul spor salonlarının ve okul servis taşıtlarının, halka açık tuvaletler kadar bakteri barındırır hale gelmesinin tahmin edilemeyecek kadar hızlı gerçekleştiğini ortaya koyuyor. Bu bağlamda bir ilaçlama firması, gerçek hijyeni yaratabilmek için en iyi ilaçlama yöntemlerini kullanmak zorunda.

ISS Haşere Kontrol uzman ekipleri her konuda olduğu gibi okullarda üst düzeyde hijyen sağlanması konusunda da ileri teknoloji ürünü ekipmanlar ve en çağdaş ürünleri kullanarak ilaçlama hizmeti veriyor. ISS, üst düzey bir ilaçlama firması olarak, çocuklarımızın günün 8-12 saati bir arada bulunduğu okullarda nano teknoloji ürünü NanoClear AG ile gerçek hijyeni sağlıyor.

NANO GÜMÜŞ FARK YARATIYOR

Nano gümüş içeren NanoClear'in en dikkat çeken özelliklerinin başında, kullanıldığı ortamlarda üç aya varan süreyle tam koruma ve pest kontrol sağlayan ilaçlama yöntemi olması geliyor. Çocukların okul, kantin, spor salonu ve servis ortamlarda hızla yayılan bulaşıcı hastalıklara yakalanma ihtimali, kokusuz ilaçlama sağlayan bu ürünle en alt seviyeye düşerken, hijyen yaratmak için kullanılan kimyasalların çocuklarda tetikleyebileceği alerji ve kanser gibi kronik riskler de ortadan kaldırılmış oluyor.

Profesyonel ilaçlama şirketi ISS Haşere Bitki Bakım uzmanları, geleneksel ilaçlama yöntemlerinin kullanıldığı temizliklerin sürekli mutasyon geçiren bakterilerde yeterince etkili olamadığına ve tam anlamıyla pest kontrol gerçekleştiremediğine, etil alkol içeren ürünlerin ise uçarak yok olduğu için sadece kısa süreliğine hijyen sağladığına dikkat çekiyor. Bu nedenle okullardaki günlük temizliği su ve Arap sabunu gibi doğal temizleyicilerle yaptıklarını vurgulayan ilaçlama firması ISS Haşere Kontrol ve Bitki Bakım, pest kontrol konusunda antibakteriyel koruma yaratmak için ise kimyasal madde içermeyen ve herhangi bir yan etkisi bulunmayan nano gümüş dezenfektan NanoClear kullandıklarının altını çiziyor.

KAMUYA AÇIK TÜM MEKANLARDA ETKİLİ

Özellikle mevsim geçişlerinde ve soğuk havalarda hızla artan salgın hastalıkların sağlığa, eğitim-öğretimin devamlılığına ve aile bütçesine yaptığı olumsuz etkiler, uzman ilaçlama firması ISS personelinin NanoClear uygulamasıyla minimuma indirgeniyor. Türkiye'de geliştirilen ve nano gümüş içeren NanoClear tek seferde hem mikropları yok ediyor hem de üç aya yakın süreyle mikrop, virüs ve mantarları ortamdan tamamen uzak tutuyor.

ISS Haşere Kontrol ve Bitki Bakım, T.C. Sağlık Bakanlığı'ndan onaylı antibakteriyel dezenfektan NanoClear AG ile en yüksek düzeyde antibakteriyel korumayı okulların yanı sıra hastaneler, toplu taşıma araçları, camiler, iş yerleri gibi kalabalık kitlelerin bir arada bulunduğu her tür mekânda aynı performansla uyguluyor.

Özel Güvenlik Çalışanları Haklarını İstiyor

300 binin üzerinde kişinin çalıştığı güvenlik sektörünün en büyük sorunu çalışan sirkülasyonu, bu da nitelikli iş gücünün bulunmasını zorlaştırıyor. Çözüm çalışan haklarının itfaiye, polislik gibi riskli meslekler benzeri iyileştirilmesi, meslek algısının oluşturulması.

Ülkemizde özel güvenlik, pek çok alanda hem vatandaş hem de kurumlar için kilit rol oynayan bir müessese. Çalışan memnuniyeti ve dolaylı olarak iş kalitesinin artması için yapılması gerekenleri Güvenlik Servisleri Organizasyonları Birliği (GÜSOD) Başkanı Murat Kösereisoğlu'ndan dinledik.

İnsan yoğun bir sektörde sürekli iş değiştiren çalışanlarla sektörün büyümesinin zor olduğunu söyleyen Murat Kösereisoğlu, "Çalışan hakları konusunu halledemezsek üstüne herhangi bir şey inşa etmek mümkün olmayacak" sözleriyle durumun ciddiyetinin altını çizdi.

Alınan eğitimlere rağmen bu sıkıntılar yüzünden sektörde ciddi bir çalışan sirkülasyonu olduğunu vurgulayan Kösereisoğlu, "Yan haklar ve tatminkar bir ücret olduğu takdirde çalışanlar sektörde kalıcı olur. Bunlardan biri bile olmadığında bırakın şirket değiştirmeyi sektör değiştiriyor çalışanlarımız" dedi. Kösereisoğlu, ağırlıklı lise mezunu olan ve yüzde 50'si nitelikli olmayan çalışanların daha az riskli endüstrilere kaymayı tercih ettiklerini kaydetti.

Yan haklar en önemli sorun

Ölüm ya da yaralanmaları "iş kazası" olarak kabul edilen güvenlik görevlileri için harekete geçtiklerini belirten Kösereisoğlu "Çalışanların malullük aylıklarının artırılması için görüşmeler yapıyoruz." dedi.

Olası bir saldırıda çatışmaya girmesi ya da şiddetli bir kavga durumunda araya girip müdahale etmesi beklenen güvenlik görevlilerinin, hayatlarını kaybetmeleri durumunda "iş kazası" kategorisinde değerlendirildiğine dikkat çeken Murat Kösereisoğlu, "İşleri gereği bu güvenlik görevlileri hep çatışma içinde olmak zorundalar. Dolayısıyla elinde cop, belinde silahla tehlikeli görevlerde çalışan bu insanların canlarına kast olması durumunda en azından kendileri ve ailelerini mağdur etmeyecek aylıklar almaları gerekiyor. Amacımız itfaiye ve polis gibi riskli mesleklere tanınan hakların özel güvenlik sektörü çalışanlarına da tanınması" dedi.

Özel çalışma grubu kuruldu

Son 3 yıldır çalışan hakları konusunda ciddi çalışmalar yürütülüyor ve çalıştaylar yapılıyor. GÜSOD bünyesinde kurdukları çalışan komitesinde bu konu üzerinde durulduğunu söyleyen Başkan Murat Kösereisoğlu, İçişleri Bakanlığı, Çalışma Bakanlığı, Emniyet Genel Müdürlüğü gibi kurumların konuya hassasiyet gösterdiğini söyledi ve ekledi: "Bizler çeşitli vesileler ile konuları farklı zeminlerde dile getiriyoruz ve getirmeye devam edeceğiz. Ben istikrarlı hükümet yönetimi, birlikte yürütülen çalışmalar dolayısıyla ümitliyim. Bu dönem zarfında gelişmeler olabileceğini düşünüyorum."

GÜSOD Üyeleri

22 yıl önce sektörün önde gelen şirketleri tarafından kurulan GÜSOD, halen 11 üyesi ve 60.000'in üzerinde çalışanıyla özel güvenlik sektörünü temsil eden en büyük dernek olma özelliği taşıyor. Dernek 2000 yılından bu yana Avrupa Güvenlik Servisleri Konfederasyonu CoESS üyesi konumunda.

Üye Şirketler

- Bantaş
- Çetin Grup
- Desmer
- Euroserve
- G4S
- ISS Proser
- Loomis
- Pronet
- Securitas
- Tav Güvenlik
- Tepe Savunma

Güvenlik çalışanların istediği haklar

Hem kendileri, hem de aileleri için güvenlikçilerin talep ettiği haklar var

- Güvenlik sektöründe asgari ücretin silahlı görevlerde %50, silahsız görevlerde yüzde 30 oranında artırılması.
- Fazla mesai ücreti çarpanının artırılması.
- Yılık izin haklarının sektöre özel artırılması.
- Tatil günlerinde çalışmaların farklı ücretlendirilmesi.
- Emniyet, Türk Silahlı Kuvvetler, İtfaiye gibi riskli işlerde çalışanlara uygulanan, emeklilik için gerekli prim gün sayısını azaltan "fiili hizmet zammı"nın güvenlik çalışanları için de uygulanması.
- Vazife başında meydana gelen kazaların ya da maluliyetlerin iş kazası olarak sınıflandırılmaması, emniyet mensuplarına uygulanan maluliyet haklarına benzer şekilde değerlendirilmesi.

“Riskli mesleklere tanınan haklar, özel güvenlik çalışanlarına da tanınmalı

Güvenlik Servisleri Organizasyonları Birliği (GÜSOD) Başkanı **Murat Kösereisoğlu**

Sosyal Medyada Başınızın Belaya Girmemesi İçin 5 Tavsiye

Çağımızın iletişim aracı olan internetin en önemli paylaşım ortamları olan sosyal medya platformları sizler ve çevrenizdekiler için pek çok risk de barındırıyor. Bilgi Teknolojileri ve İletişim Kurumu ile Telekomünikasyon İletişim Başkanlığının yayınlarında tavsiye edilen, en önemli sosyal medya davranış kurallarını paylaşıyoruz.

Get Milk
Bread
Eggs
clapton
FLOUR

1- GİZLİLİK AYARLARINIZI YAPIN!

• Paylaştığınız bilgilerin kimler tarafından görülmesi gerektiğine karar vererek gizlilik ayarlarınızı mutlaka yapın.
• Herkese açık profiliniz varsa paylaşımlarınız herkes tarafından görülür.
• Sosyal paylaşım sitelerinin kullanım şartlarını iyi öğrenerek gizlilik ayarlarınızı özelleştirin.
• Unutmayın! Gizlilik ayarları sosyal medyayı daha keyifli ve güvenli kullanmanızı sağlar.

2- ÖZEL BİLGİLERİNİZİ KORUYUN

• Bilgilerinizin kimler tarafından ne amaçla kullanılacağını bilemezsiniz. Profilinize kişisel bilgilerinizi, telefon numaranızı, ev ve iş adresinizi veya okulunuzun adını yazmayın.
• Sanal ortamda tanımadığınız kullanıcılarla arkadaş olmak, paylaştığınız bilgilerin farklı amaçlar için kullanılmasına neden olabilir.
• Profilinizde kimlerin olması gerektiğine Siz karar verin. Kullanıcıların kendilerini farklı bir kişi olarak tanıtabileceklerini asla unutmayın.

3- GÜÇLÜ BİR ŞİFRE BELİRLEYİN

• Şifreniz ne kadar güçlü olursa bir başkası tarafından çözülmesi de o denli zor olacak r. En az sekiz karakterden oluşan, tahmin edilmesi zor ve kolayca unutmayacağınız bir şifre tercih edin.
• Şifrenizin harf, sayı ve işaretlerden oluşmasına dikkat edin. Şifrenizi hiç kimseyle paylaşmayın.
• "Facebook şifresi nasıl çalınır, Twitter hesabı nasıl çalınır, Şifre kırma" gibi terimlerin her gün internete binlerce kez arandığını biliyor muydunuz?

4- SORGULAYICI BIR KULLANICI OLUN

• İnternete ulaştığınız her bilginin her zaman doğru olduğunu kabul etmeyin.
• Kredi kar bilgilerinizi veya şifrelerinizi ele geçirmek için üretilmiş kötü amaçlı yazılımların bedava oyun ve uygulama teklifleriyle yayıldığını unutmayın.
• Tanıdığınız kişilerden gelse bile tüm paylaşımlara karşı sorgulayıcı olun, emin olmadığınız içerik ve uygulamaları paylaşmayın.
• Sahte hesap ve gerçek dışı haberlere karşı dikkatli olun.

5- PAYLAŞMADAN ÖNCE BİR KEZ DAHA DÜŞÜNÜN

• Paylaştığınız her bilgi artık kontrolünüzden çıkmıştır ve geri alınamaz.

Arkadaş ortamında konuşur gibi sosyal medyada paylaşmak başınıza ciddi belalar açabilir.

Sosyal medya hesaplarınızın güvenliğini sağlamak da öncelikli tedbirlerinizden biri olmalı.

• Sosyal medyada oluşturduğunuz, paylaştığınız ve yayımladığınız her içerik, eninde sonunda halka mal olur.
• Hiç beklemediğiniz ve istemediğiniz anda karşınıza çıkartılabilir.
• İnternet üzerinden yapılan her paylaşım sonsuza kadar silinmeden kalabilir.
• Unutmayın! Şiddete teşvik, hakaret ve i ira İnternet ortamında da suçtur.

Kripto Para Madenciliğinde Büyük Tehlike!

Kripto para madenciliğinde zararlı yazılımların yayılma hızı iki kat artışla yüzde 28'e çıkarak dört kurumdan birini etkiliyor. Fortinet Tehdit Görünümü Raporu kripto paraları hedef alan zararlı yazılımların evrildiğini ortaya çıkardı.

Kapsamlı, otomatik ve entegre siber güvenlik çözümleri ile tanına Fortinet'in yeni yayımladığı Küresel Tehdit Raporu'nun sonuçları dehşet verici bazı gerçekleri ortaya koyuyor. Araştırmaya göre siber suçlular, başarılı saldırı sayısını ve bulaşma hızını artırmak için saldırı yöntemlerini evrimleştiriyor. Fidye yazılımları da kurumlara büyük zararlar vermeye devam ederken bazı siber suçluların sistemleri ele geçirerek onları fidye için tutmak yerine kripto para madenciliği için kullandığına dair belirtiler de ortaya çıktı.

SİBER SUÇLARIN SALDIRI YÖNTEMLERİ EVRİMLEŞİYOR

Siber suçluların zararlı yazılımlarını kullanırken daha iyileştiğini ve geliştiğini belirten veriler, hızlı ve ölçekli saldırı için yeni duyurulan sıfır gün açıklarını kullandığını da gözler önüne seriyor. 2018'in birinci çeyreğine göre firma başına tespit edilen saldırı yüzde 13 azalma gösterse de tespit edilen tekil saldırıların sayısı yüzde 11 artış gösterdi. Şirketlerin yüzde 73'ü de ciddi saldırılarla karşı karşıya kaldı.

MAKSİMUM ETKİ İÇİN HEDEFLİ SALDIRILAR

Suçlular yıkıcı ölçüde zararlı yazılımın etkilerini özel hedefli saldırılar ile birleştirdiği için bu saldırıların etkileri yüksek kalmaya devam ediyor. Daha fazla hedeflenen bu saldırı türleri için suçlular, kurumlara yapacakları saldırıyı başlatmadan önce önemli keşifler yapıyor. Böylece başarı dereceleri daha da yükseliyor. Devamında, ağı deldikleri anda saldırganlar, planladıkları saldırının en yıkıcı kısmını gerçekleştirmeden önce tamamen ağ geneline yayılıyorlar. 'The Olympic Destroyer' zararlı yazılımı ve yakın zamanda ortaya çıkan SamSam fidye yazılımı, siber suçluların hedefli bir saldırıyı maksimum etki için yıkıcı bir maddi yük ile birleştirdiği örneklerden bazıları.

FİDYE YAZILIMLARI AKSATMAYA DEVAM EDİYOR

Fidye yazılımlarındaki hacmin ve gelişmenin artış göstermesi, kurumlar için önemli bir güvenlik mücadelesi olmaya devam ediyor. Fidye yazılımları, tespit mekanizmalarına yakalanmadan sistemlere bulaşabilmek için sosyal medya gibi yeni bulaşma kanalları ve çok aşamalı saldırılar gibi yeni tekniklerden faydalanıyor. Ocakta ortaya çıkan GandCrab fidye yazılımı, Dash kripto parasıyla ödeme isteyen ilk fidye yazılımı olma farkına sahip. BlackRuby ve SamSam da 2018'in ilk çeyreğinde büyük tehditler olarak ortaya çıkan fidye yazılımının diğer iki türü.

SİBER HİJYEN - SADECE YAMA UYGULAMANIN ÇOK ÖTESİNDE

Sürekli iletişimin tespit edildiği ardışık günlerin sayısına bağlı olarak botnet bulaşmalarının ne kadar sürdüğü ölçüldüğünde hijyenin sadece yamalamaktan daha fazlası olduğu ortaya çıkıyor. Aynı zamanda temizlenmesi de gerek. Verilere göre botnet bulaşmalarının yüzde 58,5'i aynı gün tespit edilerek temizlendi. Yaklaşık yüzde 17,6'sı iki gün, yüzde 7,3'ü üç gün daha direndi. Yüzde 5'inin temizlemesi ise bir haftadan fazla sürdü. Örnek vermek gerekirse Andromeda botnet, 2017'nin dördüncü çeyreğinde etkisiz hale getirilse de 2018'in birinci çeyreğindeki verilerde hem hacim hem de yaygınlıkta belirgin bir şekilde kendisini gösterdi.

EVRİLEN SİBER SUÇLARLA BAŞA ÇIKMAK İÇİN ENTEGRE GÜVENLİK GEREKLİ

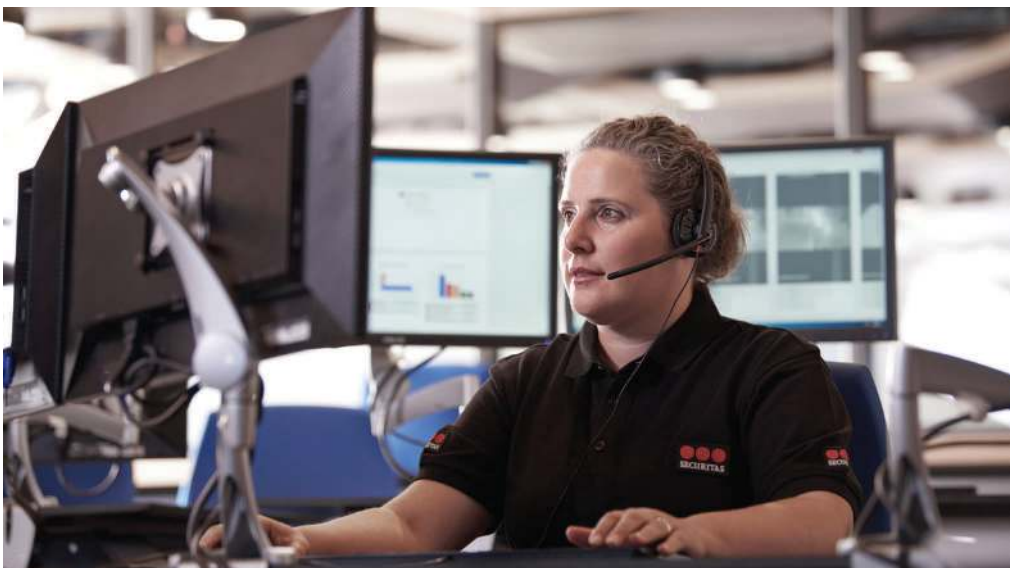
Bu çeyrek raporundaki tehdit verileri, Fortinet FortiGuard Labs 2018 küresel araştırma ekibi tarafından ortaya çıkarılan öngörü trendlerinin çoğunu destekler nitelikte olup akıllı ve otomatikleştirilmiş tehditlere karşı en iyi savunmanın entegre, kapsamlı ve otomatik güvenlik dokusu olduğunu gösteriyor. Son derece bilinçli ve proaktif bir güvenlik savunma sisteminin yeni nesil otomatik ve yapay zeka temelli saldırılara karşı ayak uydurabilmesi gerekiyor.

Securitas'tan Güvenlik 4.0 Açılımı

Endüstri 4.0 kavramıyla birlikte dönüşen hizmet anlayışına güvenlik de dahil oldu. İnsansız üretim sahalarıyla birlikte insansız güvenlik yani uzaktan izleme sistemleri artık endüstrinin hizmetinde. Securitas öncülüğü yaptığı Uzaktan İzleme Hizmetleri ile Güvenlik 4.0 dönemi başlıyor.

İnsan ve teknolojinin bir araya geldiği Securitas Entegre Güvenlik Çözümleri içinde yer alan Uzaktan İzleme Hizmetleri, teknoloji çağının en önemli sonuçlarından biri oldu.

Teknoloji uzun süredir güvenlik sektörünün de vazgeçilmez bir parçası. Geriye dönük izlemelerin yapıldığı kameralar artık yerini yeni nesil kamera ve sistemlere bıraktı. Akıllı kameralar adeta insan gözü gibi tehlikeyi algılayarak ilgili görüntüyü anında operatörün önüne getiriyor ve aksiyon alınmasını sağlıyor. Böylece hareketsiz duran bir paketi, dolaşan



şüpheli birini ya da girilmez alan olarak belirlenen yere izinsiz yaklaşanları kameralar aracılığıyla fark etmek mümkün oluyor.

Video analiz suçu oluşmadan engelliyor

Güvenlik teknolojilerindeki gelişmeleri SHIELD için değerlendiren Securitas Türkiye CTO'su Emre Erdal, akıllı video analiz yazılımları sayesinde güvenlik ihlallerini anında görüntülemenin mümkün hale geldiğini söyledi.

Bu yazılımlarla Securitas olarak sınır ve çevre ihlali, belli bir bölgede rutin olarak gezinen kişi tespiti, izinsiz

Yeni güvenlik yaklaşımı suçluyu caydırmak üzere çalışıyor

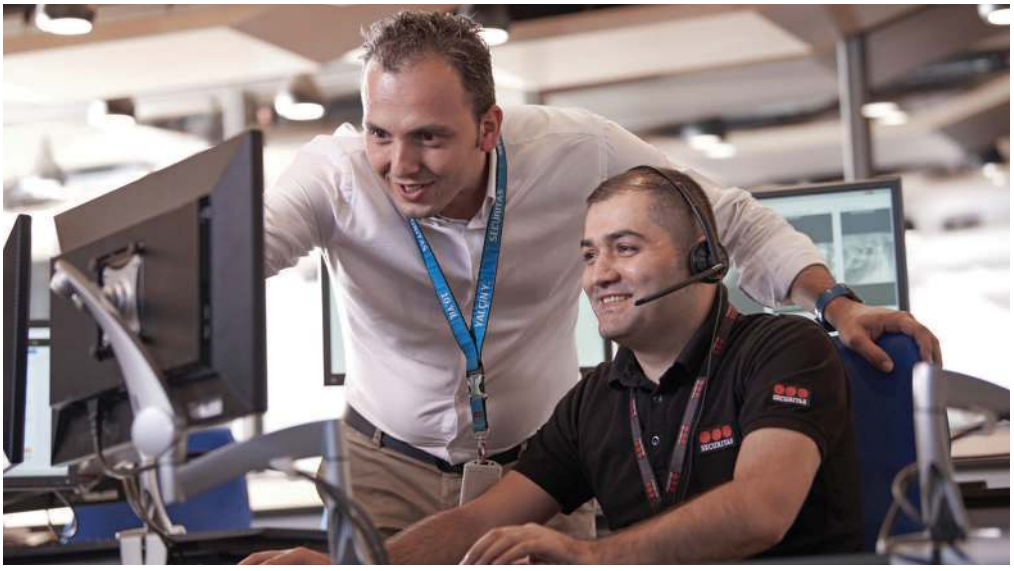
toplanma, şüpheli paket, yanlış park, ters yöne giriş gibi olumsuz durumları anında tespit edebildiklerini söyleyen Emre Erdal şunları söyledi: "Uzaktan izleme merkezimizdeki operatörün önüne ilgili alarm görüntüsünün gelmesiyle aksiyon alıyoruz. Alarm görüntüsünü alan operatör, gerekli gördüğü durumlarda uzaktan sesli anons yaparak şüphelinin suçu gerçekleştirmeden uzaklaşmasını sağlıyor. Ardından kontrol ekiplerine ve kolluk kuvvetlerine haber vererek olayı hızlıca sonuçlandırıyor. Proje maliyetlerini düşürerek riski azaltan bu sistemler müşterinin ihtiyacına göre Securitas tarafından projelendiriliyor, kuruluyor ve işletiliyor."

Türkiye'nin en büyük uzaktan izleme merkezi

Securitas, projenin büyüklüğüne göre sunduğu hizmeti farklılaştırıyor. Endüstriyel tesisler, alışveriş merkezlerine ve benzeri büyük tesislerde izleme merkezi projenin içinde kurabiliyor. Daha küçük çaplı projelerde ise İstanbul'da ve Ankara'da yer alan ve birbirinin yedeği olarak eş zamanlı çalışan Uzaktan İzleme Merkezleri aracılığıyla bu hizmetler verilebiliyor.

Böylece Türkiye'nin en büyük uzaktan izleme merkezi tarafından projelere yerleştirilen kameralar, 7 gün 24 saat izlenerek alarmlara anında müdahale ediliyor. Endüstriyel tesislerden, alışveriş merkezlerine, plazalardan, sitelere ve müstakil evlere kadar birbirinden farklı birçok alanda etkin olarak faydalanılan uzaktan izleme hizmetleri günümüzün önemli ihtiyaçları arasında yer alıyor.

İnsanlı güvenlik ile teknolojiyi bir araya getirdiklerin Securitas Entegre Güvenlik Çözümleri ile minimum maliyetlerde optimum çözümler sunuluyor.



Securitas'ın güvenlik 4.0 açılımı, insanlı güvenlik ile teknolojiyi bir araya getiriyor

Özel Sağlık Sigortası Nedir, Neleri Kapsar, Faydaları Nelerdir?

Kendinizin ve sevdiklerinizin geleceğini daha güvenli kılmak için özel sağlık sigortası en önemli tedbirlerden biri.

Kendiniz ve yakınlarınız için yakın ve uzak dönemde sağlık hizmetleri konusunda kapsamlı hizmet almak için özel sağlık sigortası büyük önem taşıyor. Basit hastalık ve kazaların yanı sıra, ciddi bazı durumlarda maliyetler çok yüksek olabiliyor. Özellikle böyle durumlar için özel sağlı sigortası yaptırmak büyük önem taşıyor.

Özel Sağlık Sigortası sigortalanan kişinin hastalıklar ve kazalar sonucu oluşacak sağlık giderlerinin karşılanması için hazırlanmış kişiye özel planlardır.

Belirlenen limitler, özel ve genel şartlar dahilinde, daha önceden sigorta poliçesinde belirtilen olası risklere karşı sigortalıyı korur. Bir özel sağlık sigortası poliçesinde en önemli unsurlardan biri genel ve özel şartlardır.

Özellikle incelenmeli ve kişiye en uygun poliçenin seçilmesi gereklidir. Genel şartlar bölümü tüm sigorta şirketleri içinde fazla farklılık göstermemesine rağmen özel şartlar bölümünde sunulan sigorta hizmetleri her sigorta şirketinde farklılık gösterir.

Özel Sağlık Sigortaları, sigortalılarına diledikleri doktor veya sağlık kurumunda tedavi olma özgürlüğü tanır. Sigorta şirketi, sigorta poliçesinin kapsamına göre sigortalının geçirdiği herhangi bir hastalık ya da bir kaza sonucunda ortaya çıkan ayakta tedavi veya yatarak tedavilerine ait masrafları karşılamayı taahhüt eder. Üstelik bunu özel şartlarda belirtti ise yurtiçi ve yurtdışı dünyanın neresinde olursa olsun karşılar. Özel sağlık sigortaları yüksek meblağlı giderleri karşılayarak sigortalının en zor anında en büyük yardımcısı olur.

ÖZEL SAĞLIK SİGORTASI NELERİ KAPSAR?

Özel sağlık sigortası, hastalık ya da kaza durumunda ödenmesi gereken sağlık masraflarını teminatlar ve limitler doğrultusunda güvence altına alır. Sağlık sigortasının genel ve özel şartları vardır. Doğru poliçeyi satın almak ve sonrasında sıkıntı yaşamamak adına poliçenin ayrıntılı bir şekilde incelenmesi gerekir.

Özel sağlık sigortası kapsamındaki tedaviler 2'ye ayrılır. Bunlar ayakta ve yatarak tedavi masraflarıdır. Tedavi masrafları sigorta şirketlerine göre değişmektedir.

Ayakta Tedavi Teminatı

Ayakta tedavi, doktor muayenesi, ilaçlar, fizik tedavi, röntgen, tahlil vs. masrafları karşılar.

Yatarak Tedavi Teminatı

Yatarak tedavi, hastanede kalmayı gerektiren tedavileri ve kemoterapi, radyoterapi vs. masrafları karşılar.

ÖZEL SAĞLIK SİGORTASININ FAYDALARI

- Özel sağlık sigortası sayesinde birçok özel sağlık kuruluşlarından az ya da hiç ücret ödemeden hizmet alırsınız.
- Bedelleri çok yüksek olan tedavi masraflarını ödemek zorunda kalmazsınız.
- Doktor ve hastane seçme şansınız vardır.
- En kaliteli hizmeti alır, kendinizi önemli hissedersiniz.
- Maddi ve manevi olarak içiniz rahat olur.

Satın aldığınız poliçeye göre yurt dışında da karşılaştığınız sağlık risklerini kapsam altına aldırırsınız.

Görüldüğü üzere sağlık

sigortasının yaptırılması önemlidir. Küçük primler sayesinde büyük masrafları ödemek zorunda kalmazsınız. Siz sağlığınıza iyi bakıyor olabilirsiniz ama her an her şeyle karşılaşılabilir.

Hiç ummadığınız bir anda kazaya maruz kalabilirsiniz bu durum sizin tamamiyle elinizde olan bir durum değildir. Dolayısıyla olası risklere karşı önlem almanız yararınıza olacaktır. Hastalığınız ya da rahatsızlığınızdan dolayı manevi çöküntü içindeyken bir de tedavi masraflarını nasıl ödeyeceğinizi düşünerek yaşayacağınız üzüntüyü sigorta yaptırarak hafifletirsiniz.

Özel sağlık sigortası fiyatları da sigorta şirketlerine göre değişmektedir. Bu fiyatı aldığınız teminat ve limitlerin etkilediği gibi kişisel bilgileriniz de etkiler. Örneğin daha önce büyük bir hastalık geçirmiş olmanız sigorta fiyatlarını yükseltir. Çünkü hastalığın tekrar etmesi riski daha fazladır. Ya da ailenizde kalıtsal bir hastalığın olması sizdeki riski de arttırdığı için fiyatlar yüksek olacaktır.

> “Kapsamlı operasyon ve tedavi gerektiren durumlarda özel sağlık sigortasının değeri daha iyi anlaşılıyor”